GROUPE INTERGOUVERNEMENTAL D'ACTION CONTRE LE BLANCHIMENT D'ARGENT EN AFRIQUE DE L'OUEST

RAPPORT REGIONAL

TYPOLOGIES DE BLANCHIMENT DE CAPITAUX ET DU FINANCEMENT DU TERRORISME LIÉS À LA CYBERCRIMINALITÉ EN AFRIQUE DE L'OUEST

Mai 2025

Le Groupe Intergouvernemental d'Action contre le Blanchiment d'Argent en Afrique de l'Ouest (GIABA) est une institution spécialisée de la CEDEAO et un organisme régional de type GAFI qui promeut les politiques de protection des États membres contre le blanchiment de capitaux, le financement du terrorisme et de la prolifération des armes de destruction massive. Les Recommandations du GAFI sont reconnues comme la norme mondiale de référence en matière de Lutte contre le Blanchiment de Capitaux, Financement du Terrorisme et de la Prolifération (LBC/FTP).

Pour plus d'informations sur le GIABA, vous êtes invités à consulter le site web : www.giaba.org

Ce document, ainsi que les données et cartes qu'il peut comprendre, sont sans préjudice du statut de tout territoire, de la souveraineté s'exerçant sur ce dernier, du tracé des frontières et limites internationales, et du nom de tout territoire, ville ou région.

Référence aux fins de citations :

Rapport de typologie du GIABA (2025), Blanchiment de Capitaux et du Financement du Terrorisme liés à la Cybercriminalité en Afrique de l'Ouest, GIABA Dakar, Sénégal.

REMERCIEMENTS

Le Directeur général tient à remercier les États membres du GIABA pour leur soutien dans la conduite de cette étude de typologies. Le GIABA est particulièrement reconnaissant à ses correspondants nationaux (CN) et aux chercheurs nationaux pour leurs efforts dans le processus de collecte de données, notamment en mobilisant les parties prenantes nationales et en facilitant un accès rapide de l'équipe de recherche avec les agences et institutions pertinentes au niveau national.

L'étude a bénéficié de l'énorme soutien des services de détection et de répression, des services de renseignement, de l'appareil judiciaire, d'autres organismes professionnels et de la société civile des États membres. Ces établissements et organismes ont veillé à ce que l'équipe de recherche rencontre les principaux intervenants et fournisse l'information requise, dans certains cas dans un délai très court.

Le GIABA tient également à souligner la collaboration exceptionnelle de nos partenaires au développement, en particulier le GAFI et l'OCWAR-C, qui ont pris le temps d'examiner le rapport à différentes étapes et de l'enrichir ainsi. Les membres du Groupe des risques, des tendances et des méthodes (RTMG) et du Groupe d'examen des politiques (PRG) du GIABA ont également travaillé en collaboration avec le Secrétariat pour améliorer la qualité globale de ce rapport.

Nous tenons également à souligner les efforts de chaque membre de l'équipe de projet, qui ont travaillé sans relâche pour assurer la coordination et l'exécution adéquates du projet, sous la supervision du directeur des politiques et de la recherche, M. Muazu Umaru. Nous remercions tout particulièrement notre collègue M. Lansana Daboh (agent de surveillance des risques) dont l'engagement a joué un rôle déterminant dans la production et la finalisation de ce rapport. Les autres membres de l'équipe de recherche qui méritent d'être soulignés sont Madame Mairo Ladidi Abass, Madame Ramatoulaye Barry Diop, M. Saer Kamara et M. Idrissa Ouattara.

Secrétariat du GIABA

TABLE DES MATIÈRES

LISTE DES ABRÉVIATIONS ET ACRONYMES

AI :	Intelligence artificielle
ML :	Blanchiment de capitaux
AML :	Lutte contre le blanchiment de capitaux
TF :	Financement du terrorisme
CFT :	Lutte contre le financement du terrorisme
PF :	Financement de la prolifération
CFP :	Financement de la lutte contre la prolifération
IoT :	Internet des objets
FIU :	Cellule d'intelligence financière
NRA :	Évaluations nationales des risques
CUA :	Commission de l'Union africaine
EFCC :	Commission des crimes économiques et financiers du Nigeria
GIABA :	Groupe intergouvernemental d'action contre le blanchiment de capitaux en Afrique de l'Ouest
CEDEAO :	Communauté économique des États de l'Afrique de l'Ouest
GEC :	Groupe d'évaluation et de conformité
RTMG :	Groupe Risques Tendances et Méthodes
PRG :	Groupe d'examen des politiques
MER :	Rapport d'évaluation mutuelle
DDOS :	Déni de service distribué
BEC :	Business Email Compromised (courriel d'entreprise compromis)
NPF :	Force de police du Nigeria
EOCO :	Office de lutte contre la criminalité économique et organisée
STR :	Déclaration de transaction suspecte
VA :	Actif virtuel
VASP :	Fournisseur de services de biens virtuels
TIC :	Technologies de l'information et de la communication
LTA :	Agence libérienne des télécommunications
FIA :	Financial Intelligent Center (centre financier intelligent)
NFIU :	Nigeria Financial Intelligent Unit (unité d'intelligence financière du Nigeria)
OCWAR-C :	Crime organisé : Réponse de l'Afrique de l'Ouest sur la cybersécurité et la cybercriminalité
GAFI :	Groupe d'action financière
NATCOM :	Commission nationale des télécommunications
BoG :	Banque du Ghana
UE :	Union européenne

RÉSUMÉ ANALYTIQUE

1. La surface d'attaque numérique s'est considérablement élargie du fait de l'évolution vers le travail à distance, de l'augmentation du nombre de personnes en ligne et de l'interconnexion accrue des ordinateurs et des appareils intelligents dans le monde entier. Avec le développement des technologies numériques, l'utilisation des réseaux d'information et de communication pour faciliter les flux financiers illicites devient l'un des principaux défis à relever pour résoudre le problème des mouvements de fonds illégaux. Les nouveaux outils numériques de transfert d'argent, tels que les services bancaires en ligne et mobiles, les paiements électroniques, les crypto-monnaies, les fournisseurs de commerce électronique et les services de jeux d'argent en ligne, surtout s'ils sont combinés, offrent un nombre incalculable d'opportunités pour éloigner l'argent de sources illégales de profit ou pour transférer illégalement de l'argent à partir de sources légales. La pandémie de COVID-19 a également créé de nouvelles opportunités pour les criminels d'abuser des systèmes financiers par le biais des technologies d'une manière plus innovante et plus complexe.

2. Au vu de ce qui précède, il est très clair que les technologies numériques posent des problèmes importants dans la lutte contre le blanchiment de capitaux, la criminalité organisée et le financement du terrorisme, car les cyber-attaques continuent d'évoluer et augmentent en fréquence et en sophistication. Tous les rapports récents du GIABA révèlent de manière flagrante la prévalence de la cybercriminalité, à la fois comme source majeure de produits du crime et comme vecteur de fonds criminels dans la région. Il apparaît que tous les types de crimes associés aux technologies numériques dans la région sont systématiquement difficiles à traiter, non seulement en raison des lacunes en matière de réglementation et d'application de la loi, mais aussi en raison du manque d'expertise et d'infrastructures adéquates. Dans la plupart des pays membres du GIABA, la cybercriminalité est une menace sérieuse pour les économies nationales qui nécessite une réponse cohérente et collaborative au niveau régional. Les normes doivent également être convenues et harmonisées au niveau international afin de réduire le risque de lacunes et d'arbitrage réglementaire.

3. Conscient de ce défi complexe, le GIABA a mené cette étude typologique sur le blanchiment de capitaux et le financement du terrorisme liés à la cybercriminalité en Afrique de l'Ouest. Malgré la gravité de ce phénomène, la cybersécurité est encore considérée comme un luxe et non comme une nécessité dans de nombreuses économies africaines. Son importance n'a pas encore été suffisamment appréciée ou reconnue. Au vu de ce qui précède, il est impératif de mener un tel exercice de typologie. Cela alimentera la base d'un fondement structurel et réglementaire de la lutte contre les crimes informatiques en Afrique de l'Ouest.

4. L'étude vise à améliorer la compréhension des risques de blanchiment de capitaux liés à la cybercriminalité dans les États membres du GIABA, afin d'améliorer la politique, la conformité et l'application. Les résultats révèleront les implications pour les interventions et des recommandations pertinentes seront proposées à cet égard. Le rapport vise à mettre en lumière les différences entre la cybersécurité et la cybercriminalité, l'ampleur des deux phénomènes en Afrique de l'Ouest et la prévalence de la criminalité. Il explorera les facteurs de risque de blanchiment et de financement du terrorisme associés à la cybercriminalité dans la région et décrira les techniques et méthodes les plus courantes adoptées pour blanchir les produits de la cybercriminalité. Il soulignera les vulnérabilités les plus critiques conduisant à des risques accrus de blanchiment des produits de la cybercriminalité et proposera des mesures politiques et des programmes orientés vers l'action qui peuvent être adoptés sur la base des résultats de l'étude.

5. La méthodologie adoptée a été une approche multipartite comprenant le Secrétariat du GIABA, des groupes d'experts et un expert des Etats membres. Les principales conclusions de l'étude comprennent une dichotomie entre la cybersécurité et la cybercriminalité, la nature prévalente des cyberaffaires et les méthodes, techniques et tendances de la criminalité en Afrique de l'Ouest. L'étude a révélé que l'Afrique de l'Ouest a connu une augmentation de la connectivité Internet supérieure à la moyenne de l'Afrique sub-saharienne. Cette connectivité est cependant

variable et dispersée. Le taux de connectivité en Afrique de l'Ouest est aussi élevé que 70% (Cabo Verde) et aussi bas que 15% (Niger). Les progrès réalisés en matière de connectivité à l'internet sont érodés par la vitesse exponentielle à laquelle la cybercriminalité est perpétrée, ce qui a des conséquences désastreuses et dommageables.

6. D'après les entretiens menés par les chercheurs nationaux, il y a une convergence de vues sur le fait que les forces de l'ordre de toute la région semblent débordées puisque deux infractions sur trois signalées sont liées à la cybercriminalité. Ce constat est d'autant plus évident que la période COVID 19 est à son apogée (2020 - 2021). Un diagramme ci-dessous au Chapitre 2 illustre la prévalence de la cybercriminalité en Afrique de l'Ouest et décrit l'ampleur (estimée) des différents types de cas perpétrés. Le type de fraude le plus répandu (40%) est celui des frais d'avance. Viennent ensuite les cas liés à l'argent mobile (15 %), puis les combines à la Ponzi (13%). Viennent enfin le piratage de sites web ou de plates-formes commerciales (7%) et la compromission de courriers électroniques d'entreprises (7%). Les cas les moins fréquents sont les fraudes à la carte de crédit/débit et les cas liés au financement du terrorisme.

7. L'on a pu identifier sept (07) différentes typologies à partir de cinquante-deux (52) études de cas qui fournissent une description complète du phénomène. Ces typologies comprennent la fraude aux cartes électroniques (crédit/débit), l'escroquerie/fraude par courrier électronique, le piratage et la fraude des systèmes des entreprises/organisations, la fraude aux avances de frais, la fraude à la pyramide de Ponzi, la fraude liée à l'argent mobile et les cas de financement du terrorisme par la cybernétique. Les indicateurs et les signaux d'alerte confirment que les informalités, le manque de sensibilisation du public aux cybermenaces, l'insuffisance des ressources investies dans la cybersécurité par les entreprises et les institutions/organisations publiques, la faiblesse de l'architecture, des systèmes réglementaires et de la surveillance du paysage cybernétique dans la région, ainsi que la faiblesse des systèmes d'application, ont un effet d'entraînement sur la cybercriminalité et la cybercriminalité assistée, le blanchiment de capitaux et le financement du terrorisme en Afrique de l'Ouest.

8. Il existe d'importantes lacunes législatives dans les pays, en particulier en ce qui concerne les pouvoirs de l'autorité centrale chargée de la lutte contre la cybercriminalité et les cadres juridiques et d'application des pays pour détecter, prouver et freiner efficacement le blanchiment de capitaux ou le financement du terrorisme associés à la cybercriminalité. Alors que les cadres juridique et répressif prévoient des mesures d'application de la loi pour enquêter sur les cybercriminels et les poursuivre, le cadre réglementaire dans la plupart des pays d'Afrique de l'Ouest prévoit des mesures préventives qui restent soit insuffisantes soit globalement faibles. Bien que quelques pays aient réalisé des progrès en matière d'administration de preuves électroniques et numériques au cours des enquêtes, cela reste un défi dans plusieurs autres pays.

9. Conformément aux exigences des normes internationales acceptables, en particulier dans le cadre de la recommandation 36 du GAFI sur la coopération internationale qui invite les pays à ratifier les instruments juridiques et autres conventions internationales pertinents tels que les Conventions de Budapest et de Malabo, la région ouest-africaine a fait des efforts et progrès considérables dans la lutte contre la cybercriminalité, ainsi que contre d'autres infractions connexes. Mais ces efforts et progrès ne sont pas exempts de défis tous azimuts tels que des lacunes dans les lois, la compréhension inadéquate des mandats des institutions, les limites capacitaires, l'inadéquation des ressources humaines et matérielles, le défaut d'une collaboration et d'une coordination optimales, de même que la faible qualité du recours à la coopération internationale.

10. Bien qu'il existe un large éventail de méthodes et de techniques utilisées par les cybercriminels pour blanchir le produit de leurs activités criminelles, les enquêteurs et les procureurs n'ont mené que peu ou pas d'enquêtes financières parallèles lorsque la cybercriminalité est détectée. Ils sont également confrontés dans de nombreux cas à la difficulté d'établir la preuve de l'infraction de cybercriminalité, en raison du manque de technologie ou d'équipement requis, de l'inefficacité de la coordination nationale intégrée entre les unités opérationnelles de lutte contre le blanchiment de capitaux et le financement du terrorisme, et de l'absence de mise en œuvre des mécanismes de coopération régionale et internationale.

11. Pour que la lutte contre la cybercriminalité soit plus efficace et dissuasive, l'étude propose quelques recommandations à l'intention du public et des autorités compétentes qui luttent contre la cybercriminalité. Il est nécessaire de lancer et d'intensifier les campagnes de sensibilisation du public, de promouvoir la culture de la cybersécurité dans la région et d'aider les pays à mettre en place un cadre juridique et institutionnel conforme aux normes internationales en vigueur. Procéder à une évaluation appropriée des risques et mettre en place un laboratoire de criminalistique numérique pour fournir des preuves médico-légales aux autorités chargées de l'application de la loi. Renforcer les capacités opérationnelles des enquêteurs en matière de techniques d'investigation numérique et combler le fossé entre le cadre juridique et les lois spéciales sur la lutte contre le blanchiment de capitaux, le financement du terrorisme et le financement du terrorisme, afin de faciliter et d'accélérer les poursuites pénales en cas de délit cybercriminel.

12. Mettre en place un forum régional des plateformes nationales de lutte contre la cybercriminalité en Afrique de l'Ouest afin de permettre aux autorités compétentes de travailler en réseau, de partager des informations et des renseignements. Suivre la signature, la ratification et la transposition dans le droit national des instruments internationaux et renforcer les capacités en matière de détection, d'enquête, de poursuite et de jugement des affaires de cybercriminalité, ainsi que la manière de suivre l'argent, y compris en menant des enquêtes parallèles et financières.

CHAPITRE 1

INTRODUCTION

Contexte

13. Les technologies émergentes telles que les voitures autonomes, l'intelligence artificielle (IA), l'apprentissage automatique, l'automatisation, la virtualisation, les villes intelligentes, les réseaux Blockchain, le Big Data, l'Internet des objets (IoT), l'Internet des sens, l'informatique en nuage et l'informatique quantique, etc. créent des changements opérationnels qui nécessiteront de nouvelles exigences en matière de cybersécurité. Au cours des deux dernières années, la surface d'attaque numérique s'est considérablement élargie en raison du passage au travail à distance, de l'augmentation du nombre de personnes en ligne et de l'interconnexion accrue des ordinateurs et des appareils intelligents dans le monde entier.

14. Simultanément, les entreprises criminelles ont profité du manque de visibilité et de l'absence d'administration de la sécurité. Avec le développement des technologies numériques, l'utilisation des réseaux d'information et de communication comme outil de facilitation des flux financiers illicites augmente. Et cela devient un des principaux défis à relever pour résoudre le problème des mouvements de fonds illicites. Il va sans dire que les technologies numériques facilitent les flux financiers illicites à chaque étape, qu'il s'agisse de gagner de l'argent illégalement, de transférer des fonds illégaux ou de les utiliser. Il existe plusieurs domaines dans lesquels des liens clairs peuvent être établis entre la technologie et les flux financiers illicites.

15. Outre la création des marchés illégaux souterrains de la cybercriminalité et de la criminalité cybernétique, les technologies numériques facilitent la migration de la criminalité organisée traditionnelle en ligne et offrent plusieurs possibilités de fraude, de corruption, d'évasion fiscale entre autres activités criminelles. Les nouveaux outils numériques de transfert d'argent, tels que les services bancaires en ligne et mobiles, les paiements électroniques, les crypto-monnaies, le commerce électronique et les jeux d'argent en ligne, offrent un nombre incalculable d'opportunités pour éloigner l'argent des sources illégales de profit ou pour transférer illégalement de l'argent à partir de sources légales, surtout s'ils sont combinés.

16. En outre, les nouvelles formes de commerce en ligne et l'économie numérique facilitent le transfert de profits illégaux et l'agrégation de fonds illicites sur des comptes offshore, ainsi que leur placement dans de fausses sociétés de commerce électronique et des entreprises en ligne offshore. La pandémie de COVID-19 a également créé de nouvelles opportunités pour les criminels d'abuser des systèmes financiers par le biais des technologies d'une manière plus innovante et plus complexe.

17. Au vu de ce qui précède, il est très clair que les technologies numériques posent des problèmes importants dans la lutte contre le blanchiment de capitaux, la criminalité organisée et le financement du terrorisme, car les cyber-attaques continuent d'évoluer et augmentent en fréquence et en sophistication. C'est la raison pour laquelle la cybercriminalité est devenue un domaine d'attention et d'investissement majeur dans le monde entier.

18. En Afrique de l'Ouest, le lien entre le blanchiment de capitaux et le financement du terrorisme (BC/FT) et la cybercriminalité est flagrant. Si le BC/FTBC/FT s'est répandu du fait de la mondialisation financière (c'est-à-dire la capacité de tous les acteurs économiques et sociaux à utiliser des services financiers au niveau international), la cybercriminalité quant à elle se développe grâce à la mondialisation technologique à travers le développe-

ment d'Internet et des outils qui y sont liés. Le rapport du GIABA sur le déploiement des Fintech, les gros titres des journaux, les rapports d'activité annuels soumis par les États membres du GIABA et leurs rapports sur les évaluations nationales des risques de blanchiment de capitaux et de financement du terrorisme, les résultats des évaluations mutuelles et les processus de suivi, révèlent tous de manière flagrante la prévalence de la cybercriminalité, à la fois comme source majeure de produits du crime et comme vecteur de fonds d'origine criminelle dans la région. Il apparaît que tous les types de crimes associés aux technologies numériques dans la région sont systématiquement difficiles à traiter, non seulement en raison des lacunes en matière de réglementation et d'application de la loi, mais aussi en raison du manque d'expertise et d'infrastructures adéquates.

19. Dans la plupart des pays membres du GIABA, la cybercriminalité est une menace sérieuse pour les économies nationales qui nécessite une réponse cohérente et collaborative au niveau régional. L'incapacité de certaines juridictions à lutter contre la cybercriminalité menace la sécurité, la stabilité et l'efficacité des gouvernements, des infrastructures critiques, des entreprises et des individus dans toute la région. Il faut donc une gouvernance résiliente, qui garantisse la coopération des agences concernées dans toutes les juridictions (par exemple, entre les superviseurs, les CRF et d'autres organes opérationnels chargés de la prévention de la criminalité ou de l'application de la loi). Les normes sur le plan national doivent également être convenues et si possible harmonisées au niveau régional voire international afin de réduire le risque de lacunes et d'arbitrage réglementaire, notamment dans une perspective de maitrise des flux transfrontaliers. Evidemment, le manque de cohérence et d'harmonisation entre les juridictions entraine des coûts de mise en conformité.

20. Conscient de ce défi complexe, le GIABA a mené cette étude typologique sur le blanchiment de capitaux et le financement du terrorisme liés à la cybercriminalité en Afrique de l'Ouest.

Motivation de l'étude

21. La plupart des économies africaines se caractérisent par la permissivité des régimes réglementaires, ce qui constitue un terrain fertile pour les activités de cybercriminalité. Selon un rapport de novembre 2016 de la Commission de l'Union africaine (CUA) et de la société de cybersécurité Symantec, sur les 54 pays d'Afrique, 30 ne disposaient pas de dispositions légales spécifiques pour lutter contre la cybercriminalité et traiter les preuves électroniques. Dans certains pays, les responsables de l'application de la loi ne prennent pas de mesures significatives contre les pirates informatiques qui s'attaquent aux sites web internationaux. Par exemple, certains fonctionnaires nigérians ont affirmé qu'ils n'étaient pas au courant des cybercrimes provenant du pays, tandis que d'autres les ont qualifiés de propagande occidentale. Certains hauts fonctionnaires élus seraient également impliqués dans la cybercriminalité. En 2003, la Commission des crimes économiques et financiers du Nigeria (EFCC) a arrêté un membre de la Chambre des représentants du Nigeria pour son implication présumée dans des activités liées à la cybercriminalité.

22. Le classement des affaires de cybercriminalité en fonction des pays d'origine (AUC, 2016) des plaignants fait apparaître trois pays africains parmi les 50 plus touchés : il s'agit de l'Afrique du Sud, qui occupe la 11e place (434 plaintes), du Nigeria (24e place, avec 215 plaintes) et de l'Égypte (45e, avec 95 plaintes). Lorsque les affaires sont catégorisées en fonction des dommages causés, les plaignants sud-africains sont à nouveau en première position avec 6,5 millions de dollars perdus, suivis par le Nigeria (2,9 millions de dollars) et l'Egypte (523.000 dollars). L'émergence de ces délits liés aux transactions par téléphone est rendue plus accessible par la généralisation des moyens de paiement par mobile money.

23. Quant à la fraude à la Sim box, elle a coûté 926 millions de francs CFA à la Côte d'Ivoire en 2014. Cette technique permet aux fraudeurs de contourner les canaux habituels des télécommunications internationales, qui sont alors traitées comme des appels locaux, aboutissant ainsi à des opérations d'arbitrage de taux. Cela entraîne des pertes énormes pour les entreprises de télécommunications. Au Sénégal, bien que peu de données soient disponibles, le cas le plus significatif concerne une société de transfert d'argent dont le site web a été piraté pendant plusieurs heures en 2020. Les pirates, qui se disaient sénégalais, voulaient attirer l'attention sur la question de

la sécurité. La page d'accueil du site comportait une page noire avec un texte des deux auteurs. Ils disent, entre autres, que la cybersécurité est hélas négligée dans le pays et que leur action était entreprise pour rappeler l'importance de la cybersécurité aux personnes concernées.

24. Malgré la gravité de ce phénomène, la cybersécurité est encore considérée comme un luxe et non comme une nécessité dans de nombreuses économies africaines. Son importance n'a pas encore été suffisamment appréciée ou reconnue. Dans de nombreuses organisations, les budgets consacrés à la cybersécurité seraient inférieurs à 1 %, et beaucoup d'organisations n'ont pas de budget alloué à la cybersécurité. Pourtant, les technologies numériques ont le potentiel de servir d'outil pour s'attaquer au problème du blanchiment de capitaux et du financement du terrorisme. Elles peuvent être une source d'autonomisation et de transparence, et pourraient être utilisées dans les enquêtes, la détection et la perturbation des transferts illégaux d'argent.

25. Compte tenu de ce qui précède, il était impérieux de procéder à une étude de typologie approfondie. Cela permettra de jeter les bases d'une structure et d'une réglementation robustes de la lutte contre la criminalité informatique en Afrique de l'Ouest. Elle permettra également de mettre en lumière les menaces probantes de la cybercriminalité et la mesure dans laquelle celle-ci facilite d'autres infractions principales liées au blanchiment de de capitaux et au financement du terrorisme dans la région du GIABA.

Objectif

26. L'étude des typologies vise à améliorer la compréhension des risques de blanchiment de capitaux liés à la cybercriminalité dans les États membres du GIABA, afin d'améliorer la politique, la conformité et l'application. Les résultats révèleront les implications pour les interventions et des recommandations pertinentes seront proposées à cet égard. Le rapport aborde les questions spécifiques suivantes :

a) Quelles sont les différences entre la cybersécurité et la cybercriminalité ? Et quelle est l'ampleur de ces deux phénomènes en Afrique de l'Ouest ?
b) Quelles sont les différentes formes d'activités criminelles utilisant les technologies numériques dans les États membres du GIABA ?
c) Quels sont les facteurs de risque de blanchiment de capitaux et de financement du terrorisme associés à la cybercriminalité dans la région ?
d) Quelles sont les techniques et méthodes les plus courantes adoptées pour blanchir les produits de la cybercriminalité en Afrique de l'Ouest ?
e) Quelles sont les vulnérabilités (systémiques) les plus importantes entraînant des risques accrus de blanchiment des produits de la cybercriminalité ?
f) Quelles sont les mesures politiques et les programmes orientés vers l'action qui peuvent être adoptés sur la base des résultats de l'étude pour atténuer efficacement les risques de blanchiment de capitaux et de financement du terrorisme associés aux technologies numériques ?

Méthodologie de l'étude

27. En prélude à la méthodologie, l'étude a été conçue par suite de plusieurs réunions d'échange et de discussions lors des forums techniques du GIABA et des réunions de ses différents groupes de travail (RTMG/PRG et réunions des experts et de l'ECG) - discussions au cours des séances d'adoption des REM, rapport d'évaluation Fintech, évaluation des risques en particulier VA & VASP) entre 2022 et début 2021. La méthodologie détaillée adoptée par la suite comprend les éléments suivants :

- Une **session de réflexion de trois jours** a été organisée en **juillet 2021** afin de réfléchir aux principaux problèmes liés à cette question ainsi qu'au champ d'application du projet. La session a pris en compte les présentations des représentants des États membres sur la situation actuelle de la cybercriminalité dans leurs pays respectifs. Les membres du RTMG/PRG ont également contribué à cet effet.

- Une session virtuelle de brainstorming s'est tenue en **septembre 2021** et les résultats de ces deux (2) sessions ont permis de finaliser le concept du projet et les termes de référence détaillés pour recruter les membres de l'équipe du projet dans les États membres du GIABA.

- Une équipe de projet a été constituée, composée de 15 chercheurs nationaux (un expert recruté dans chaque Etat membre de la CEDEAO), des membres du RTMG et du PRG du GIABA, et soutenue par le Secrétariat du GIABA en **juillet 2022**.

- Collecte et analyse des données (administration des questionnaires, y compris la conduite d'entretiens approfondis avec un éventail d'autorités compétentes, d'agences de lutte contre la cybercriminalité, d'institutions financières ainsi que de victimes de cybercriminalité et d'autres personnes vulnérables) - (**juillet-septembre 2022**).

- Examen des rapports nationaux soumis par les experts et analyse approfondie des modèles, des méthodes, des techniques et de l'impact du phénomène, ainsi qu'une analyse critique des résultats, y compris le suivi au niveau national, le cas échéant (septembre-octobre **2022**).

- Examen des rapports nationaux lors de l'atelier annuel du GIABA sur l'exercice des typologies régionales (**octobre 2022**).

- Rédaction d'un rapport complet, comprenant des recommandations spécifiques et générales qui aideraient à la formulation de politiques et d'interventions opérationnelles contre le BC/FT lié à la cybercriminalité aux niveaux national et régional - (**mars-avril 2023**).

- Traduction et revue de qualité du projet de rapport consolidé dans les 3 langues de la CEDEAO - **avril - mai 2023**.

- Examen et validation hors site par les États membres, les observateurs, les partenaires de développement, les membres du RTMG/PRG et d'autres parties prenantes - **mai 2023**.

- Examen et approbation du rapport par la plénière du GIABA - **mai 2023**.

Source : Liberia

CHAPITRE 2

LA PRÉVALENCE DE LA CYBERCRIMINALITÉ EN AFRIQUE DE L'OUEST

28. Ce chapitre tente d'examiner et de présenter l'étendue et les types de cybercriminalité perpétrés dans la région de l'Afrique de l'Ouest, compte tenu du volume de cas de cybercriminalité signalés quotidiennement et de l'incapacité des forces de l'ordre à enquêter sur chaque cas. Il convient également de noter que le nombre de cas ou d'incidents signalés aux forces de l'ordre ne se traduit pas nécessairement par une enquête, car plusieurs cas ou incidents signalés (des dizaines et des centaines de rapports) peuvent être liés et aboutir à un seul cas. Ce chapitre examinera certaines questions contextuelles et de définition avant d'aborder les types de cas prévalant dans la région, tels qu'ils ont été signalés.

Dichotomie entre cybercriminalité et cybersécurité

29. La cybercriminalité est une activité criminelle qui implique un ordinateur, un dispositif de réseau ou un réseau, visant directement à endommager ou à désactiver des ordinateurs et des dispositifs, à diffuser des logiciels malveillants par exemple, à voler des informations secrètes, etc. Il y a cybercriminalité lorsqu'un ordinateur, un dispositif de réseau ou un réseau est (a) pris pour cible, ou (b) accessoirement utilisé pour commettre le crime, ou (c) utilisé directement pour perpétrer le crime. Alors que (a) et (b) sont largement dus à des vulnérabilités du système, (c) est une menace directe pour le système. En outre, alors que le point a) concerne le niveau d'alerte, de sensibilisation et de préparation du public (toutes les personnes physiques et morales) en matière de cybersécurité, le point b) concerne la capacité politique, réglementaire et répressive à prévenir et à perturber la cybercriminalité, y compris la gestion efficace de l'architecture et de l'environnement cybernétique de la juridiction (domaine public).

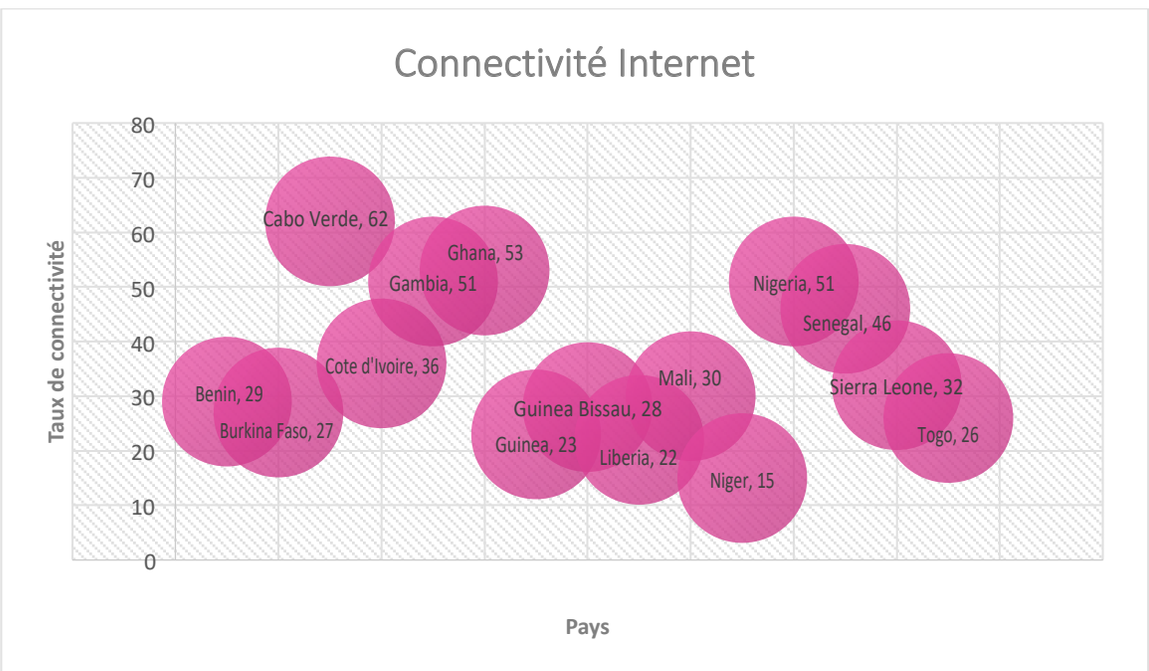
30. La cybersécurité est la technologie et le processus conçus pour protéger les réseaux et les appareils contre les attaques, les dommages ou les accès non autorisés. La cybersécurité vise à protéger les organisations, ce qui permet d'accroître l'efficacité et la productivité et d'inspirer confiance aux clients/partenaires. Les aspects de la cybersécurité comprennent la protection des données et la sécurisation des systèmes d'une organisation afin de prévenir les attaques. La cybersécurité est une exigence opérationnelle importante pour tout acteur économique et surtout nécessaire pour trois (3) raisons principales, à savoir les principes de confidentialité (les informations et les fonctions ne doivent être accessibles qu'aux parties autorisées), d'intégrité (les informations et les fonctions ne doivent être ajoutées, modifiées ou supprimées que par les parties autorisées) et de disponibilité des informations (les systèmes, les fonctions et les données doivent être disponibles à la demande selon des paramètres convenus basés sur les niveaux de service).

31. Prévenir et réprimer la cybercriminalité constitue une importante fonction de la cybersécurité. En effet, le processus permettant de s'assurer qu'un système informatique est protégé contre toute forme d'intrusion ou d'abus ne se limite pas à la mise en place de plusieurs niveaux d'authentification et de mots de passe complexes, de pare-feu et d'antivirus avec cryptage sur des serveurs de noms de domaine sécurisés, mais aussi à des mises à jour régulières et à l'évaluation des risques (identifier, surveiller et évaluer les menaces), et à la mise en place de mesures d'atténuation pour les risques identifiés. Bien que la cybersécurité puisse contribuer à prévenir certaines formes de cybercriminalité, toutes les formes d'infractions cybernétiques ne peuvent pas être évitées uniquement grâce à une bonne cybersécurité.

Prévalence de la cybercriminalité en Afrique de l'Ouest

32. Bien que l'étude (dans le chapitre suivant) présente les différentes typologies observées en Afrique de l'Ouest, cette section présente la prévalence du crime sans plonger dans les techniques et méthodes détaillées utilisées pour perpétrer le crime. L'Afrique de l'Ouest a connu une augmentation de la connectivité Internet supérieure à la moyenne de l'Afrique sub-saharienne. Cette connectivité est cependant variée et dispersée. Le taux de connectivité en Afrique de l'Ouest peut atteindre 70 % (Cabo Verde) et 15 % (Niger). Les progrès réalisés grâce à la connectivité à l'internet ont entrainé la vitesse exponentielle à laquelle la cybercriminalité est perpétrée. Ses conséquences sont désastreuses et dommageables. Le diagramme ci-dessous (figure 2.1) montre le taux de connectivité à l'internet dans la région.

Figure 2.1 : Connectivité Internet en Afrique de l'Ouest



33. D'après les entretiens menés par les chercheurs nationaux, il y a une convergence de vues sur le fait que les forces de l'ordre de toute la région semblent débordées puisque deux infractions sur trois signalées sont liées à la cybercriminalité. Ce constat est d'autant plus évident que la période COVID 19 est à son apogée (2020 - 2021). Le diagramme ci-dessous illustre la prévalence de la cybercriminalité en Afrique de l'Ouest et décrit l'ampleur (estimée) des différents types de cas perpétrés. Le type de fraude le plus répandu (40%) est celui des frais d'avance. Viennent ensuite les cas liés à l'argent mobile (15 %), puis les combines à la Ponzi (13 %). Viennent enfin le piratage de sites web ou de plates-formes commerciales (7%) et la compromission de courriers électroniques d'entreprises (7%). Les cas les moins fréquents sont les fraudes à la carte de crédit/débit et les cas liés au financement du terrorisme.

Figure 2.2 : Prévalence et type de crime en Afrique de l'Ouest

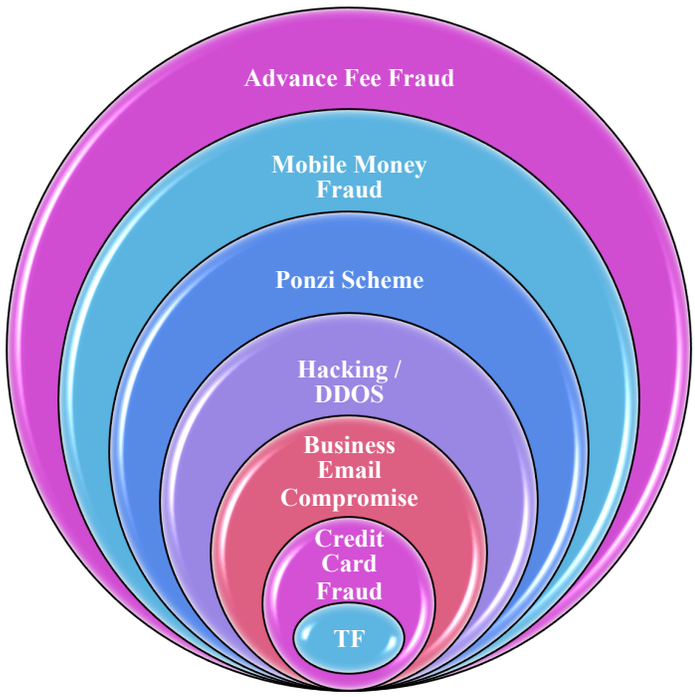


Tableau 2.1 : Prévalence et type de crime avec moyenne pondérée en Afrique de l'Ouest

Type de crime	Moyenne pondérée	Description spécifique / titre de l'infraction
Fraude à l'avance de frais	0.39	Escroquerie à l'or, sextorsion, pédopornographie, extorsion, escroquerie à la romance, escroquerie au recrutement, escroquerie à la proposition commerciale, escroquerie au contrat d'exportation, escroquerie au service de fret, escroquerie à l'héritage, traite des êtres humains et enlèvement, falsification et chantage, fraude et usurpation d'identité.
Fraude à l'argent mobile	0.15	Faux-semblants, usurpation d'identité et falsification, fraude à la carte SIM, délit d'initié et piratage, fraude à l'agent de téléphonie mobile, usurpation d'identité par le biais d'une carte SIM préactivée, abandon du registre des électeurs.
Fraude à la Ponzi	0.14	Système de trading en ligne, fraude à la Ponzi, système de Ponzi sur les actifs virtuels, escroquerie à l'investissement en ligne / au marché des valeurs mobilières, système de Ponzi sur l'investissement en argent mobile, escroquerie à l'investissement dans le commerce électronique, escroquerie au prêt en ligne.
Piratage/ DDOS	0.12	Piratage de site web, piratage de plate-forme commerciale, DDOS, délit d'initié/employé compromis, piratage de compte de médias sociaux et usurpation d'identité, délit d'initié et système de facilité de crédit frauduleux.
Compromission du courrier électronique d'une entreprise	0.10	BEC, phishing et escroquerie par courrier électronique
Fraude à la carte de crédit	0.06	Vol de cartes de crédit ou de débit, fraude à la carte de crédit ou de débit
En rapport avec la TF	0.06	Fonds de commerce, soupçons de collecte de fonds pour le fonds de commerce, hawala pour le fonds de commerce

CHAPITRE 3

TYPOLOGIES ÉTUDES DE CAS SUR LE BLANCHIMENT DE CAPITAUX ET FINANCEMENT DU TERRORISME LIES A LA CYBERCRIMINALITÉ EN AFRIQUE DE L'OUEST

34. Ce chapitre traite des différentes typologies observées à partir des cas identifiés présentés ici. Il y a 52 cas appartenant à sept typologies différentes, présentées ci-dessous. Ces typologies comprennent la fraude aux cartes électroniques (crédit/débit), l'escroquerie/fraude par courrier électronique, le piratage et la fraude aux systèmes des entreprises/organisations, la fraude aux avances de frais, la fraude à la pyramide de Ponzi, la fraude liée à l'argent mobile et les cas de financement du terrorisme par la cybernétique.

Typologie 1 : Fraude aux cartes électroniques (crédit/débit)

35. Trois cas ont été identifiés dans cette typologie à partir des cas soumis. Il s'agissait de fraude électronique, de vol de données de cartes de crédit ou de débit et d'incitation des victimes à payer pour des produits inexistants par le biais d'un marketing en ligne frauduleux.

Cas 1 : Fraude à la carte de crédit/débit et utilisation de la société Shell

Une source a déposé une plainte auprès de la FIUL pour fraude électronique et blanchiment de capitaux de la part de Korlane Investment Limited Liability Company et de ses propriétaires. La LEA a mené une enquête approfondie sur cette allégation. Les enquêteurs ont découvert que Korlane Investment Limited Liability Company exploitait une société écran au Liberia, sans bureau, sans personnel, etc., et qu'elle avait ouvert et utilisé ses comptes au Liberia pour blanchir, dissimuler et diriger des fonds volés générés par des transactions inhabituelles provenant d'une fraude électronique - un délit préalable au blanchiment de capitaux. Les suspects ont été inculpés de blanchiment de capitaux, de vol de biens, de fraude électronique et d'association de malfaiteurs.

Après avoir obtenu un mandat d'arrêt du procureur, les auteurs se sont soustraits à l'arrestation et ont fui le pays. Une requête en confiscation des produits a été déposée conformément à la loi de 2013 sur les recours provisoires en matière de produits de la criminalité. La requête a été assignée pour audition et plaidée. Le tribunal a fait droit à la requête et a ordonné la confiscation du produit de la criminalité, soit plus de 234 000 USD, et son transfert au GOL. La technique utilisée par le cybercriminel consistait à se servir de cartes de crédit de la plateforme E-Money (swift, Visa et MasterCard) pour effectuer des transactions frauduleuses. Le criminel a manipulé la carte MasterCard pour dépasser le seuil de la banque. Ce type de fraude est connu sous le nom de fraude internationale à la carte de crédit et n'est pas conforme aux normes de MasterCard.

Source : Liberia

Cas 2 : Fraude à la carte de crédit/débit et fausse transaction d'importation/exportation

L'accusé, propriétaire d'une société spécialisée dans les produits agricoles et l'outillage agricole, a ouvert quatre comptes auprès d'une banque donnée. Entre le 24 janvier 2017 et le 31 mars 2017. L'accusé, qui était impliqué dans des fraudes à la carte de crédit, a créé un site web de marketing en ligne, par l'intermédiaire duquel il a reçu plusieurs commandes, principalement des États-Unis, pour la fourniture de produits agricoles. L'accusé s'est inscrit sur la plateforme de paiement en ligne de la banque, qui permet à des clients peu méfiants d'effectuer des paiements directement sur son compte pour les marchandises commandées. En l'espace de deux mois, l'accusé a reçu sur son compte 1 468 447,59 GHS (341 500 USD) provenant de plusieurs cartes de crédit de différentes juridictions. Cependant, sa banque a reçu des demandes de remboursement de Visa et de MasterCard de la part de la Bank of America, indiquant que certains des paiements effectués en faveur de la société n'avaient pas été autorisés par les propriétaires des cartes et qu'ils étaient donc frauduleux. Au cours des vérifications effectuées par la banque, l'accusé a prétendu que les fonds provenaient de l'exportation de produits agricoles qu'il avait expédiés à des clients par l'intermédiaire d'agences de transport maritime.

Les enquêtes ont toutefois révélé que les agences maritimes mentionnées n'avaient pas expédié ces produits et que les factures de fret aérien présentées à l'appui de ses affirmations étaient toutes fausses. Une déclaration d'opération suspecte (DOD) a donc été déposée auprès du FIC. L'accusé, mécontent de la décision de la banque de conserver les fonds, a dénoncé la banque à l'EOCO pour avoir conservé ses fonds sans justification. À l'insu de l'accusé, l'EOCO avait déjà reçu des informations de la FIC pour enquêter sur l'accusé. L'enquête de l'EOCO a collaboré avec le FBI et le SFO pour entrer en contact avec les victimes et un dossier prima facie a été établi contre l'accusé, indiquant que les cartes de crédit à partir desquelles les paiements ont été reçus par l'accusé étaient des cartes volées.

En conséquence, l'accusé a été inculpé de fraude fiscale, de blanchiment de capitaux et d'escroquerie par faux semblants. Au cours des poursuites, cinq des victimes ont témoigné par vidéoconférence via Skype pour confirmer qu'elles n'avaient pas acheté de marchandises à l'accusé et que leurs cartes de crédit avaient été utilisées frauduleusement. À l'issue des poursuites, l'accusé a été condamné à une amende de 1 000 unités de pénalité, soit 12 000 GH¢ (2 390 USD), ou, à défaut, à cinq ans d'emprisonnement.

Source : Ghana

Étude de cas n° 3 : vol de cartes de crédit/débit et usurpation d›identité

Une compagnie de téléphone, afin d'améliorer ses services, a opté pour des transactions internationales d'un compte bancaire vers un compte électronique. Cette innovation a reçu un accueil favorable et a permis à l'entreprise d'enregistrer de bons résultats. Cependant, elle a reçu une alerte l'informant de l'existence de transactions internationales frauduleuses, effectuées de la France vers la Côte d'Ivoire. L'affaire a été signalée à l'agence chargée de la lutte contre la cybercriminalité (PLCC) afin d'appréhender les responsables. De l'enquête ouverte à la suite du signalement, il ressort que dès réception des dépôts illicites, les numéros bénéficiaires effectuent immédiatement les retraits.

Les investigations menées par le PLCC en collaboration avec le Laboratoire de criminalistique numérique (LCN) ont permis de découvrir les suspects grâce à leurs numéros de téléphone portable. Le premier suspect, AAJ, a été arrêté avec l'aide d'une unité de ladite société. Lors de l'interrogatoire, il a reconnu avoir reçu plusieurs dépôts d'argent sur son compte en provenance de France. Il a poursuivi en disant qu'un de ses correspondants rencontrés sur Facebook lui a demandé d'effectuer des retraits à hauteur de dix pour cent (10%) des montants retirés. Il termine en précisant que ce correspondant Fabino ne lui a donné aucun détail, et qu'il lui suffisait de retirer l'argent et de le remettre à un proche. Des investigations complémentaires ont conduit à l'arrestation de M. Fabino à son domicile à Abidjan. La perquisition a permis de découvrir plusieurs cartes de crédit/débit associées à des banques françaises et n'appartenant pas à Fabino. Lors de l'interrogatoire, Fabino a déclaré qu'il était responsable de 16 dépôts pour un montant total de 2 290 344 FCFA, soit 3 524 euros, alors qu'il se trouvait en France, sur les numéros de son ami AAJ. Fabino était également responsable de plusieurs retraits effectués sur le compte bancaire français. L'affaire était en cours au moment de la présente étude.

Source : Côte d'Ivoire

Typologie 2 : Escroquerie / Fraude par courriel compromis

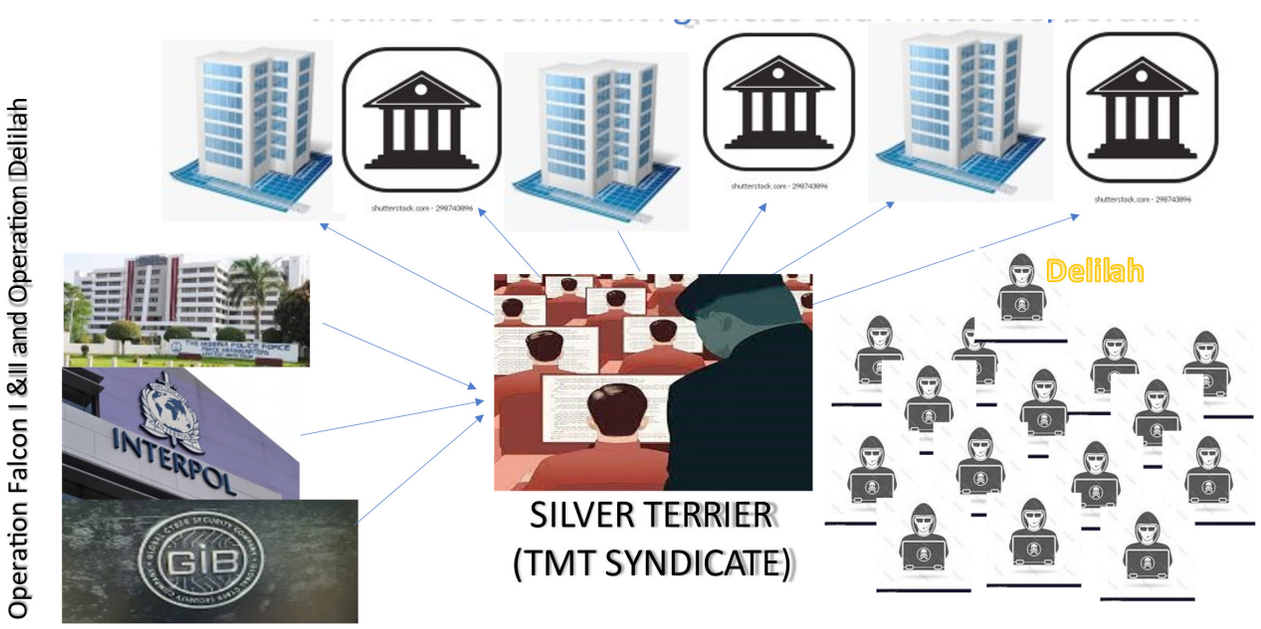
36. Cette typologie est pratiquée depuis un certain temps et très populaire en Afrique de l'Ouest. Les criminels utilisent un logiciel d'ingénierie pour envoyer de faux courriels à des victimes potentielles dans le monde entier. Une fois que vous avez cliqué sur ces courriels et/ou commencé à communiquer avec eux, ils peuvent avoir accès à des informations sensibles concernant votre courriel et votre entreprise, tout en utilisant ces informations pour vous frauder ou vous escroquer, vous et les membres immédiats de votre réseau.

Cas 1 : Le courrier électronique d'une entreprise est compromis par une fraude organisée

La police nigériane a arrêté 11 membres présumés d'un réseau de cybercriminalité prolifique dans le cadre d'une opération de police nationale coordonnée avec INTERPOL. Arrêtés par des agents de l'unité de police spécialisée dans la cybercriminalité des FNP et du Bureau central national (B.C.N.) d'INTERPOL au Nigéria, bon nombre des suspects seraient membres de « SilverTerrier «, un réseau connu pour ses escroqueries de type « business email compromise « (BEC) qui ont fait du tort à des milliers d'entreprises dans le monde entier. Au cours de l'opération Falcon II, qui a duré dix jours (du 13 au 22 décembre), 10 agents du PFN ont été déployés du siège d'Abuja à Lagos et Asaba afin d'arrêter les suspects ciblés, identifiés à l'avance grâce aux renseignements fournis par INTERPOL. Les opérations sur le terrain ont été précédées d'une phase d'échange et d'analyse de renseignements, au cours de laquelle le Nigéria a utilisé le réseau mondial de communication policière sécurisée d'INTERPOL, I-24/7, pour travailler avec les services de police du monde entier qui enquêtent également sur des escroqueries à la fausse monnaie liées au Nigéria. Le Secrétariat général d'INTERPOL a soutenu les opérations sur le terrain 24 heures sur 24, 7 jours sur 7, en procédant à l'extraction et à l'analyse des données contenues dans les ordinateurs portables et les téléphones mobiles saisis par la police nationale lors des arrestations. Cette analyse préliminaire indique que la participation collective des suspects à des systèmes criminels de type BEC pourrait être associée à plus de 50 000 cibles. L'un des suspects arrêtés était en possession de plus de 800 000 identifiants de domaines de victimes potentielles sur son ordinateur portable. Un autre suspect surveillait les conversations entre 16 entreprises et leurs clients et détournait des fonds vers «SilverTerrier» lorsque des transactions de l'entreprise étaient sur le point d'être effectuées. Un autre individu est soupçonné d'avoir participé à des opérations de BEC dans un grand nombre de pays d'Afrique de l'Ouest, dont la Gambie, le Ghana et le Nigeria.

Source : Nigeria

Titre : version française *(à envoyer)*



Méthodes et techniques

- Développement de noms de domaine, de liens d'hameçonnage et de campagnes de publipostage massives.
- Développement/acquisition de programmes malveillants/espions et d'outils d'accès à distance.
- Il s'est livré à l'usurpation d'identité, à l'usurpation d'identité et à la falsification de documents.
- Utilisation d'entreprises tierces pour déplacer et détourner les fonds extorqués aux victimes.
- L'utilisation des commerces de façade.

Drapeaux rouges et indicateurs

- Transactions financières inhabituelles.
- Changement soudain de mode de vie, de l'humble entrepreneur d'une start-up à la vie luxueuse et tape-à-l'œil.
- Fonds reçus sur un compte dont le nom du bénéficiaire est différent de celui du compte.

Cas 2 : Phishing et escroquerie par courrier électronique

L'enquête de police a établi que le plaignant, le 1er décembre 2021, a ouvert un compte de messagerie électronique Wawo-NGO à l'adresse «wawoliberia@yahoo.com»a été manipulé (hameçonnage) et un courriel malveillant a été envoyé au plaignant, wawoliberian@yahoo.com («n» a été ajouté à l'email original) aurait été utilisé pour communiquer avec son donateur «DED» et a emporté la somme de 20 500,00 USD qui a été transférée via la Bank-B le 15 novembre 2021 d'un donateur partenaire DED et a également utilisé un numéro orange (0775000....) sur whatsApp dans une conversation prétendant être le responsable de programme de l'ONG Wawo qui s'est présenté comme responsable financier et un numéro de téléphone mobile 0777028... assigné à un compte d'argent mobile dont le nom d'utilisateur est «BM-1» a été attaché au compte e-mail de l'ONG Wawo qui a été supprimé par la suite après avoir autorisé l'accès au compte e-mail de l'ONG Wawo. La technique utilisée était le piratage (hameçonnage) du compte de messagerie et l'envoi d'un courriel malveillant à un donateur pour lui demander des fonds. Un courriel compromis aurait été utilisé pour demander des fonds au donateur «DED» et établir d'autres liens de communication (Whatsapp) pour authentifier la transaction. Le pirate a réussi à faire passer le compte bancaire de la banque A à la banque B. Le système de blanchiment de capitaux utilisé dans ce cas est la falsification et le vol de biens. Les personnes impliquées étaient le personnel de Wawo-NGO et un pirate informatique inconnu. Cette affaire fait l'objet d'une enquête depuis le 28 décembre 2021.

Source : Liberia

Cas 3 : Fraude et usurpation d'identité par courriel d'entreprise

Le service de lutte contre la cybercriminalité de la police nigériane, basé au Bureau central national INTERPOL (B.C.N.) d'Abuja, a reçu un rapport du gouvernement allemand, par l'intermédiaire du bureau du procureur général et du ministre de la Justice, faisant état d'une escroquerie au courrier électronique dans le cadre de l'achat de masques de protection COVID-19. Des fraudeurs non identifiés ont gagné la confiance d'un intermédiaire en Irlande en initiant des transactions commerciales portant sur des produits médicaux. En négociant habilement avec l'intermédiaire et en présentant des contrats de livraison et des factures contrefaits, les fraudeurs ont fait croire à l'intermédiaire qu'il serait en mesure de livrer de grandes quantités de masques de protection COVID-19 pour les autorités gouvernementales allemandes. Au final, des acomptes d'un montant de plus de 2,3 millions d'euros ont été versés sur un compte bancaire aux Pays-Bas, et des paiements partiels d'un montant de 498 000 euros avaient déjà été transférés sur un compte bancaire de première génération au Nigeria sur instruction d'un Nigérian, Babatunde Adesanya alias Teddy A, qui avait donné à l'avance des instructions sur ce qu'il convenait de faire de l'argent. Musterpoint Investment Nig Ltd, une société domiciliée auprès d'une banque de première génération au Nigeria, était la destination des 498 000 euros en question. Cependant, grâce à la coopération internationale des services chargés de l'application de la loi, la banque a été contactée par INTERPOL et le transfert a été interrompu, l'argent étant renvoyé à son point d'origine. Cette affaire a conduit à l'arrestation de deux suspects par l'unité de lutte contre la cybercriminalité de la police nigériane, qui font actuellement l'objet de poursuites devant la Haute Cour fédérale du Nigéria.

Source : Nigeria

Cas 4 : Fraude au courrier électronique d'entreprise compromis

Les 5 et 12 février 2018, une banque commerciale a effectué deux virements respectivement de 50 000 euros et 145 000 euros en faveur de deux (02) sociétés. Ces transferts étaient réputés avoir été autorisés par l'un de ses clients qui dispose d'un accord de banque en ligne avec la banque et qui a toujours instruit ses transferts par email. La banque a reçu les instructions par email pour les deux transferts en question et a reçu un autre email par lequel le client modifiait les coordonnées bancaires des bénéficiaires. Les différents Swift des deux virements ont été produits et lui ont été envoyés après exécution. Les transferts n'ont pas été contestés jusqu'au 20/02/2018 où le vrai client est revenu pour dire que s'il avait autorisé les transferts, il n'avait en revanche donné aucune instruction pour modifier les coordonnées des bénéficiaires des fonds transférés. La banque a découvert par la suite qu'un cybercriminel avait pu accéder au système de la banque et avait introduit ces modifications de destinataires avec de faux courriels dans le processus de transfert. L'affaire était en cours au moment de la présente étude.

Source : Togo

Cas 5 : Fraude au courrier électronique d'entreprise compromis

La CRF a reçu un rapport d'usurpation d'identité de la part d'Hibiscus, une organisation non gouvernementale locale. Elle attendait son deuxième versement de fonds d'un montant total de 707 841,12 NLe, destinés aux populations clés affectées à l'intérieur du pays, de la part de ses partenaires internationaux, Gardenia Help. Les fonds ont été frauduleusement détournés vers un autre compte portant le même nom, Hibiscus, auprès d'une autre banque WY. Les enquêtes internes d'Hibiscus ont révélé que le courrier électronique du directeur de programme avait été piraté et qu'il était le principal canal de circulation des informations pertinentes entre les fraudeurs et les partenaires internationaux. Les activités d'Hibiscus ont été suspendues par Gardenia jusqu'à ce que l'affaire soit résolue.

Les investigations de la CRF ont révélé qu'un compte Hibiscus frauduleux avait bien été ouvert à la banque WY et que les fonds d'un montant total de 707 841,12 NLe avaient bien été transférés directement de Gardenia Help.

Les fonds ont été immédiatement transférés sur un autre compte de Sunflower Tech dans la même banque et retirés dans les trois jours par le seul signataire de Sunflower Tech. Les enquêtes ont également révélé qu'il existait un lien direct entre l'ASBL Hibiscus frauduleuse, Sunflower Tech et son signataire. La banque WY n'a pas fait preuve de la diligence requise et n'a pas pris les mesures KYC nécessaires lors de l'ouverture du compte Hibiscus frauduleux. Si elle l'avait fait, elle aurait détecté tous les signaux d'alarme. Elle était plus préoccupée par la rentabilité.

Les ONG Gardenia Help et Hibiscus NPO ont des connaissances très limitées en matière de blanchiment de capitaux et de financement du terrorisme, ce qui rend leurs systèmes internes poreux et facilement accessibles aux fraudeurs au sein de leurs organisations. Le bénéficiaire final a été appréhendé par l'ACC et l'enquête est en cours.

Source : Sierra Leone

Typologie 3 : piratage et fraude des systèmes d'une entreprise ou d'une organisation (site web/base de données)

37. Une autre typologie populaire est le piratage et la prise de contrôle du site web, de la plateforme ou de la base de données d'une entreprise ou d'une organisation à l'aide de techniques d'ingénierie et de logiciels très sophistiqués. Les techniques ne sont pas très différentes des attaques de logiciels malveillants ou de logiciels rançonneurs. Cependant, en Afrique de l'Ouest, les criminels ne s'affichent guère pour demander une rançon. Ils sont soit payés pour le faire par des rivaux ou des concurrents, soit, dans le cas d'institutions financières, la plateforme où les transactions sont effectuées est prise en charge pour exécuter des transferts et des paiements illégaux avant que les victimes ne puissent le détecter et faire des efforts pour reprendre le contrôle de leur système. Il arrive que les délits d'initiés fassent partie du modus operandum.

Cas 1 : Piratage du système d'une entreprise ou d'une organisation (DDOS et fraude)

Cybercriminel britannique, M. Kaye a attaqué une société libérienne de téléphonie mobile et a involontairement interrompu l'Internet du Liberia - en 2016. Kaye, originaire d'Egham dans le Surrey, est un pirate informatique autodidacte qui a commencé à vendre ses compétences considérables sur le dark web - offrant aux individus des opportunités de cibler et de détruire leurs rivaux commerciaux. Selon les documents du tribunal, Kaye a été engagé en 2015 pour attaquer une grande société de téléphonie mobile et de fourniture d'accès à Internet, par un individu travaillant pour son rival et principal concurrent. Rien n'indique que l'entreprise rivale était au courant de l'action de l'employé, mais l'individu a offert à Kaye jusqu'à 10 000 dollars (7 800 livres sterling) par mois pour qu'il utilise ses compétences afin de détruire l'entreprise, de jeter le discrédit sur ses services et de nuire à sa réputation.

Les utilisateurs de téléphones portables ont commencé à voir leurs appareils se déconnecter. L'entreprise a fait appel à des consultants en cybersécurité qui ont tenté de repousser l'attaque, mais il était déjà trop tard car le réseau de zombies était devenu incontrôlable. L'internet au Liberia dépendait à la fois d'un petit nombre de fournisseurs et d'un câble atlantique relativement limité. Kaye avait envoyé une telle quantité de trafic à l'entreprise que l'ensemble du cyber-système national s'est bloqué. Selon les enquêteurs, l'internet du pays est tombé en panne à plusieurs reprises entre le 3 et le 4 novembre 2016, perturbant non seulement l'entreprise attaquée, mais aussi des organisations, des petites entreprises et des utilisateurs individuels dans tout le pays. Les actions de M. Kaye ont empêché les clients de l'entreprise de communiquer entre eux, d'accéder aux services essentiels et de mener à bien leurs activités quotidiennes. Un nombre important de clients sont passés au principal concurrent.

M. Kaye a reconnu avoir commis un délit d'utilisation abusive d'un ordinateur en lançant des cyber-attaques contre une entreprise au Libéria, et d'avoir été en possession du produit d'un délit (10 000 dollars trouvés sur lui lors de son arrestation). Au cours des années précédant les attaques par déni de service distribué (DDOS), le chiffre d'affaires annuel de la société dépassait 80 millions de dollars (62,4 millions de livres sterling). Après l'attaque, le chiffre d'affaires a diminué de plusieurs dizaines de millions et le passif de l'entreprise a augmenté, lui aussi, de plusieurs dizaines de millions de dollars américains.

Source : Liberia

Cas 2 : Piratage du système d'une entreprise ou d'une organisation (DDOS et fraude)

En 2020, une institution financière a signalé à la police que des cybercriminels avaient compromis l'ensemble de son système bancaire et avaient un accès total à son système bancaire central. Les cybercriminels ont modifié les numéros de référence des transactions passées et injecté une somme totale de 48 000 000 D (857 142,8 USD) sur différents comptes. Les pirates ont également levé la limite de retrait quotidien des distributeurs automatiques de billets de la banque, permettant ainsi aux titulaires de comptes (acteurs locaux/conspirateurs/accompagnateurs) de retirer autant d'argent que possible. Les pirates lancent des requêtes sur le système bancaire et suppriment tous les historiques de transactions illégales, de sorte que les transactions sur les comptes concernés ne pouvaient pas être consultées à partir du système frontal de la banque, mais seulement à partir du commutateur Gam Sarver de la banque centrale.

Le titulaire du compte (acteurs locaux/complices) a réussi à retirer (à l'aide d'un distributeur automatique de billets) 7 000 000 D (125 000 USD) et une enquête plus approfondie a révélé qu'une partie de l'argent avait été envoyée au Ghana, en Afrique du Sud et au Sénégal. Cependant, grâce à la coopération internationale (Interpol et CRF), une partie des fonds envoyés au Ghana a été récupérée sur le compte d'une société et la totalité des fonds envoyés au Sénégal a également été récupérée.

Il est également important de reconnaître qu'à l'époque de cette enquête, le pays ne disposait pas d'un laboratoire de criminalistique numérique pour examiner les appareils. Bien qu'aucun des pirates n'ait été arrêté, 23 suspects, complices des pirates, ont été arrêtés. L'enquête a été conclue et l'affaire a été transmise au procureur général pour avis.

Source : Gambie

Cas 3 : Piratage du système d'une entreprise ou d'une organisation (DDOS et fraude)

Au cours du mois de juillet 2020, la Brigade Centrale de Lutte contre la Cybercriminalité a reçu une instruction par le biais d'une lettre envoyée par le Procureur du Tribunal de Grande Instance 1st de Ouagadougou, de mener une enquête approfondie sur l'accès frauduleux et l'entrave au fonctionnement d'un système informatique, la modification de données informatiques, l'association ou l'entente en vue de commettre des infractions informatiques, le vol d'argent liquide, le blanchiment de capitaux et de proposer des charges contre toute personne impliquée dans les infractions susmentionnées.

L'enquête a révélé que dans la nuit du dimanche 21 au lundi 22 juin 2020, des pirates informatiques ont attaqué une plateforme électronique d'argent mobile à travers un réseau téléphonique. Ils ont attaqué cinq (05) comptes principaux de la plateforme et celui d'une banque de la place où était hébergée et gérée la plateforme d'argent mobile. Les pirates ont effectué des transferts frauduleux pour un montant total de quatre-vingt-dix-neuf millions cent quatre-vingt-sept mille cinq cent soixante-dix-neuf (99 187 579) FCFA. Ces transferts ont été effectués vers plusieurs numéros de téléphone, titulaires de comptes de mobile money dans le pays et vers d'autres numéros dans 3 autres pays voisins. Le montant total des comptes que les pirates ont pu bloquer, tant au niveau national qu'international, s'élève à plus de trois cent quatre-vingt-un millions (381.000.000) de FCFA.

L'enquête a permis d'arrêter plusieurs suspects qui ont été déférés au procureur de la 1ère Haute Cour pour suite à donner.

Source : Burkina Faso

Cas 4 : Blanchiment (superposition) par l'intermédiaire d'un employé de banque compromis

Du 20 au 29 septembre 2022, une banque commerciale de Bissau a signalé que des opérations frauduleuses de transfert en ligne avaient été effectuées par des inconnus qui n'étaient pas des employés de la banque. Selon des sources de la CRF et de la police, les transferts ont été effectués depuis le compte de la banque vers des comptes de clients de la même banque.

À la suite de l›enquête, la police judiciaire, avec l›aide de l›unité chargée de la conduite criminelle et de l›escroquerie et de l›unité nationale de lutte contre la criminalité économique, a demandé la coopération des sociétés de télécommunications pour suivre les communications effectuées au cours du mois écoulé, à l›aide de certains téléphones portables (6 numéros SIM) soupçonnés d›être impliqués dans l›affaire. Mme Y, la suspecte du site 1st , a coopéré avec la police sur son implication dans le comportement criminel de fraude et d'abus de confiance.

Mme Y a avoué être titulaire d'un compte d'épargne domicilié à la banque XPTO à Bissau, mais à la demande de son mari M. X, elle a communiqué son numéro de compte à un ami Mario, qui avait besoin d'un compte lié à une carte VISA à la banque XPTO. Sans aucune diligence, M. X a fourni les détails du compte à son ami Mario. Quelques jours plus tard, Mme Y a indiqué avoir reçu un message sur son téléphone portable indiquant une opération de crédit d'un montant de six cent quarante-huit mille cent quarante et un francs CFA (648 141 FCFA). Elle a ensuite mis sa carte de débit VISA à la disposition de son mari qui, par l'intermédiaire de son ami, a encaissé l'argent en plusieurs fois.

Quelques jours plus tard, le compte est à nouveau crédité de la somme de cinq millions de francs CFA (5 000 000 FCFA). Cette fois, l'ami de son mari lui a demandé de se rendre au guichet de la banque pour effectuer un retrait direct, qui devrait être annoncé à l'avance, mais en raison de la relation de son mari avec l'un des employés, elle a pu retirer la totalité de la somme en une seule fois. Elle a ensuite reçu un appel du PK, qui lui a demandé de retourner à la banque afin de clarifier la situation concernant le retrait indu qu'elle a effectué et les anomalies survenues sur son compte.

L'enquête est toujours en cours. Toutefois, il convient de noter l'existence de défaillances dans le système de contrôle des transferts électroniques de fonds au niveau de la banque référencée et dont les cybercriminels en collaboration avec certains employés de la banque ont profité pour effectuer des transferts illégaux en dehors du fonctionnement normal de la banque. L'affaire a également révélé les vulnérabilités du système de contrôle au niveau des banques et des établissements financiers, ainsi que les menaces de cybercriminalité auxquelles le pays est confronté, notamment, en l'absence d'infrastructures et de capacités techniques pour faire face à ces menaces.

Source : Guinée Bissau

Cas 5 : Piratage d'un compte de média social, usurpation d'identité et escroquerie

Une victime, Mary T., a signalé à la police qu'un individu se faisant passer pour son oncle avait demandé, par l'intermédiaire de son compte de messagerie Facebook, de transférer 800 dollars américains et 75 000 dollars libanais à un numéro donné le 11 mai 2022. Le pirate a créé un compte de messagerie Facebook en utilisant le nom complet de son oncle. L'idée était que l'oncle avait un besoin urgent d'argent pour régler certaines obligations au Libéria et que l'argent lui serait remboursé par la suite. Après avoir été convaincue et sur la base de la confiance accordée à son oncle, elle a effectué un transfert du montant via MoneyGram depuis les États-Unis, conformément aux instructions. Le criminel a piraté le compte de messagerie de la victime et s'est fait passer pour son oncle, demandant un transfert d'argent et envoyant un message demandant à la victime de transférer de l'argent à un numéro donné. Les infractions préalables au blanchiment de capitaux sont la fraude et l'extorsion/le vol de biens perpétrés par un individu et un pirate informatique inconnu. Dans ce cas, la victime a reçu un message prétendument envoyé par son oncle lui demandant de transférer des fonds sur un compte mobile money. L'affaire fait l'objet d'une enquête.

Source : Liberia

Cas 6 : Délit d'initié, système organisé et frauduleux de facilité de crédit

La CRF a reçu un rapport (enquête de retour de fraude) sur un déboursement suspect de crédit non autorisé de la Jimpex Commercial Bank (JCB). 150 clients de la JCB se sont vu accorder frauduleusement des facilités de découvert sans aucun document, pour un montant de 54 484 754 082,47 Le (équivalent à 0.5 dollars américains).

Le responsable des rapports de portefeuille de JCB et le chef de division intérimaire (gestion des risques de crédit) ont été les cerveaux qui ont mis au point ce système illégal. Ils ont ensuite impliqué dans le projet le personnel informatique qui avait accès aux données.

Le Credit Risk Manager a utilisé son code d'accès spécial pour autoriser des découverts à des clients présélectionnés de JCB. Le Credit Risk Manager a soigneusement sélectionné des clients existants de la banque qui exploitaient des entreprises crédibles et les a incités à participer à la manœuvre illégale. Chacun des bénéficiaires du système illégal a été invité à fournir un montant spécifié en espèces aux conspirateurs avant de pouvoir accéder à la facilité de découvert illégale. Après paiement du montant demandé, le Credit Risk Manager autorisait la facilité de découvert en utilisant son code d'accès. Le personnel de l'ICT qui faisait partie de la combine a également fermé les yeux.

L'enquête de la TOCU a permis d'établir un lien entre quatre maisons ultramodernes nouvellement construites et une flotte de voitures de luxe, d'une part, et le gestionnaire du risque de crédit et le responsable des rapports de portefeuille, d'autre part. Le gestionnaire du risque de crédit est en fuite tandis que l'enquête se poursuit.

Source : Sierra Leone

Typologie 4 : Fraude à l'avance et blanchiment de capitaux

38. Il s'agit toujours de l'infraction principale la plus commise en Afrique de l'Ouest. Elle représente plus de 40 % des cas signalés ici. L'avance de frais est soit basée sur une escroquerie amoureuse, une sextorsion, des demandes d'héritage ou des propositions commerciales, soit sur une combinaison de deux ou plusieurs des méthodes mentionnées. Une autre méthode unique qui mérite d'être soulignée est la fraude à l'avance de frais réalisée derrière les barreaux d'une prison, avec des fonctionnaires de la prison comme complices.

Cas 1 : Arnaque à l'or et fraude à l'avance de frais

La police a enquêté sur cette affaire à la suite d'une plainte déposée par deux hommes d'affaires britanniques. En 2020, les deux investisseurs britanniques et leurs partenaires commerciaux ont été présentés par une connaissance en ligne à M. «A», un Ghanéen, comme un homme d'affaires spécialisé dans le commerce de l'or. Les investisseurs ont manifesté leur intérêt pour l'achat de lingots d'or auprès de M. «A» et se sont ensuite rendus au Ghana, à l'invitation de M. «A», qui leur a également demandé de le rencontrer en personne pour négocier la transaction. En février 2020, M. «A» et un complice, M. B, ont rencontré les investisseurs et leur ont montré 20 kilogrammes de lingots d'or.

Les investisseurs étrangers se sont déclarés prêts à acheter cinq kilogrammes d'or, pour lesquels M. «A» et son complice ont exigé et perçu 69 000 dollars à titre de paiement partiel initial de la valeur de l'or. Après avoir reçu l'argent, ils ont promis d'exporter l'or aux investisseurs, qui en prendraient livraison à Dubaï, dans les Émirats arabes unis. Mais ils n'ont finalement exporté qu'un seul kilogramme d'or aux investisseurs. M. «A» a expliqué qu'il n'avait pas pu exporter la quantité d'or nécessaire en raison de retards dans le processus de documentation par les fonctionnaires des douanes à l'aéroport international de Kotoka et qu'il avait promis d'exporter la quantité restante aux investisseurs le 3 décembre 2020, mais qu'il ne l'avait pas fait. Il a ensuite demandé 130 000 dollars, soit le solde du paiement pour les quatre kilogrammes d'or, et a demandé 70 000 dollars supplémentaires aux investisseurs pour garantir l'exportation du reste de l'or. N'ayant pas honoré sa parole, il a indiqué qu'il n'avait pas pu exporter l'or, car il n'y avait pas de compagnies aériennes pour exporter l'or en raison de la pandémie de COVID-19.

M. A a également affirmé que la lettre de voiture destinée à faciliter l'exportation de l'or ne pouvait être acceptée par la Precious Minerals Marketing Company, car la quantité était trop faible, et qu'il ajouterait donc cinq kilogrammes d'or supplémentaires pour porter le total à 10 kilogrammes afin de faciliter l'exportation. En juillet 2020, M. A a annoncé aux investisseurs qu'il avait été arrêté par INTERPOL et des représentants de certaines agences de sécurité et que les lingots d'or avaient été confisqués.

Pour faciliter la remise de l'or, il a exigé diverses sommes d'argent et a ensuite indiqué que les barres d'or avaient été remises à l'Economic and Organised Crimes Office (EOCO), qui exigeait 300 000 dollars avant de lui remettre le précieux minerai. Les investisseurs ont envoyé les 300 000 dollars à M. A, portant le montant total qui lui avait été envoyé à 1 075 000 dollars, mais il n'a pas tenu sa promesse, ce qui a conduit à son arrestation. Il a ensuite été inculpé de complicité d'escroquerie par faux semblants, d'escroquerie par faux semblants et de vente et d'achat de minéraux sans licence. Le procès est actuellement en cours.

Source : Ghana

Cas 2 : Sextorsion, pédopornographie et extorsion de fonds

En 2016, un cas a été signalé à la police concernant trois personnes : Flavio, Filipe et Steve. Les suspects ont créé un faux profil sur les médias sociaux sous le nom de «Maurice Marcovich», utilisé à des fins criminelles. Ils ont utilisé cette fausse page pour envoyer des demandes d'amitié à leurs victimes potentielles, qui étaient pour la plupart mineures au moment des faits. Après avoir échangé quelques messages via Facebook Messenger, ils ont commencé à menacer de mort les victimes, leur famille et/ou leurs proches s'ils ne se montraient pas dans des poses pornographiques, en prenant des photos et des vidéos avec leurs propres téléphones portables et en les forçant à les envoyer via Messenger.

Après avoir vu les photos et les images des victimes lors des entretiens viachat da Internet -Messenger, le «faux profil» sous le nom de «Maurice Marcovich», leur ordonne d'envoyer une demande d'amitié à «Flávio Yolo Alves», «Rui Filipe Alves» et «Steve Aristides Santos», sur Facebook.

Cependant, par cette ruse, ils ont effrayé et contraint les victimes à les rencontrer et à pratiquer des actes sexuels, en les filmant avec leurs téléphones portables et ceux des victimes, ce qu'elles ont accepté en raison de la peur qu'ils leur ont inspirée, soit par des menaces, soit par la divulgation publique de leurs photos et vidéos pornographiques qu'ils possédaient déjà.

Les victimes ont été menacées, non seulement par la publication de photographies et de vidéos, mais aussi par l'envoi d'une photo d'une arme à feu à charger, accompagnée des messages suivants : «tu ne vas plus m'ignorer», «je tue tous les jours», «je sais beaucoup de choses sur toi», «parce que je veux ton sang», «demain tu peux être sûr que tu n'auras plus de vie», «je suis un trafiquant de drogue international en Syrie, au Brésil et en France», «et j'ai déjà ordonné l'assassinat de plusieurs étudiants en Irak», etc. Ils ont également envoyé aux victimes des photographies de leurs proches, prises dans des lieux publics et à proximité de leur domicile, afin de les intimider et de les effrayer davantage.

Face à ces menaces de mort insistantes, les victimes, désespérées et effrayées, ont accédé aux prétentions de ces individus et ont envoyé d'autres photographies et vidéos, obscènes et indécentes, montrant leurs parties intimes ainsi que leurs visages.

Ces individus, parfois individuellement ou en groupe, organisaient des rencontres avec les victimes dans différents endroits et les forçaient à avoir des relations sexuelles avec eux, et les actes étaient filmés et photographiés, affirmant qu'ils avaient reçu l'ordre de «Maurice Marcovich» de faire tout cela et de l'envoyer.

Au cours de ces actes de violence contre ces victimes, l'une d'entre elles, âgée de moins de 13 ans, est tombée enceinte, et les preuves recueillies ultérieurement, basées sur la collecte de l'ADN des suspects aux fins de l'identification de la paternité, ont prouvé que «Rui Filipe Alves» était le père.

Insatisfaits des actions ci-dessus, ils sont toujours sous la menace constante, utilisant le faux profil «Maurice Marcovich», ont forcé certaines victimes à se prostituer et, en conséquence, ont reçu l'argent de cette pratique, qu'ils ont facturé à chaque client, un montant entre 5 et 7 mille escudos, approximativement 50 à 70 Euros/Dollars.

Les individus «Flávio Yolo Alves» et «Rui Filipe Alves» ont été arrêtés et présentés à la Cour. Lors du jugement, Flávio a été condamné à 33 ans de prison et Rui à 14 ans.

Source : Cabo Verde

Cas 3 : Utilisation d'une société fictive ou d'une société écran et fraude à l'avance de frais

En 2009, M. A, qui est commerçant, ouvre un compte dans la banque X pour des raisons liées à ses activités commerciales. Mais sur ce compte, il ne reçoit que des virements en provenance de l'étranger. Quatre ans plus tard (2013), son épouse ouvre un compte dans la même banque, toujours pour des raisons professionnelles. Le compte de cette dernière a reçu sur la période de 2013 à 2019, 48 virements pour un total de122 282 518 FCFA. Une seule opération de paiement a été effectuée sur le compte. Mais de manière surprenante, Monsieur A contrôle le compte de son épouse dans son intégralité. Tous les retraits ont été effectués par lui-même et généralement immédiatement après chaque réception. En 2014, il se constitue en société et ouvre un troisième compte dans le même établissement bancaire. Dans les mêmes conditions, il bénéficie de 114.905.014 FCFA entre 2014 et 2019. Tous ces faits ont conduit la banque X à faire une déclaration de soupçon à la CENTIF. En 2018, il ouvre un autre compte dans une seconde banque Y et reçoit un virement d'une banque nigérienne, pour un montant total de 189 500 000 FCFA qui s'est avéré être un virement frauduleux obtenu à la suite d'une attaque du système informatique de la banque. Mais grâce à la

vigilance de cette dernière, les fonds ont pu être restitués à la banque Y avant que M. X n'entre en possession des sommes. La banque Y envoie immédiatement une DOS à la CENTIF. Les investigations de la CENTIF révèlent que M. X est le petit frère d'un cyber-escroc connu de ses bases de données. Il fait partie d'un réseau de cyber-criminels qui se livrent à des escroqueries de type nigérian (scam 419). Leur méthode consiste à utiliser des sociétés écrans et des intermédiaires ou des prête-noms pour attirer leurs victimes en leur proposant des affaires très lucratives. Au passage, ils créent des coûts imaginaires que la victime doit payer, notamment les frais d'étude du dossier, les frais juridiques, les frais de comptabilité, etc. Ce manège leur a permis de soutirer 451.615.304 CFA à leur victime. Suite aux enquêtes, M. X a été reconnu coupable de blanchiment de capitaux, d'escroquerie en bande organisée et d'atteinte à la sécurité informatique et condamné à 72 mois de prison dont 12 avec sursis et à une amende de 100.000.000 CFA. Sa femme a été reconnue coupable de blanchiment simple et condamnée à 36 mois de prison, dont 12 avec sursis, et à une amende de 50 000 000 CFA. Il y a eu confiscation de 11.481.787 FCFA saisis sur un de leurs comptes et confiscation d'une voiture leur appartenant au profit de l'Etat.

Source : Togo

Cas 4 : Escroquerie au romantisme et fraude à l'avance de frais

M. A, un citoyen ghanéen qui s'est fait passer pour une femme afin d'escroquer un ressortissant australien de 43 ans, M. X, dans le cadre d'une escroquerie à la romance, a été condamné à 10 ans d'emprisonnement. Dans ses relations avec la victime, M. A s'est fait passer pour une femme sous une fausse identité en ligne et a rencontré la victime sur un site de rencontre. La victime est un pêcheur commercial à la retraite et un citoyen australien. La victime a indiqué qu'après avoir rencontré l'escroc en ligne, M. A l'a convaincue d'acheter une propriété au Ghana et de soutenir financièrement la famille supposée de M. A. En conséquence, il a remis un montant total de 115 000 dollars australiens à l'accusé au Ghana par le biais de virements bancaires.

La victime, se rendant compte qu'elle était victime d'une escroquerie, a déposé une plainte auprès de l'EOCO et lui a demandé de mener une enquête sur l'escroquerie présumée. L'accusé a été appréhendé en décembre 2017 et a ensuite été traduit devant la Haute Cour pour escroquerie par faux semblants, blanchiment de capitaux et possession de documents falsifiés. En juin 2018, l'accusé a été reconnu coupable des charges retenues contre lui et condamné à 10 ans d'emprisonnement avec travaux forcés. Un montant de GHS52000 (USD11,000) en souffrance sur son compte a été gelé et remis à la victime.

Source : Ghana

Cas 5 : Escroquerie au recrutement et aux avances de frais

En 2022, les enquêtes dans cette affaire ont eu pour origine plusieurs plaintes déposées auprès des organes de police criminelle (OPC), de la police judiciaire et de la police nationale, où certaines victimes rapportent qu'elles ont reçu une invitation via le réseau social. FACEBOOK, d'un profil avec une photographie du ministre des Affaires étrangères et des Communautés du Cap-Vert, et d'autres disent avoir reçu une invitation d'un profil du vice-ministre du Premier ministre et du ministre des Finances à laquelle ils ont accepté en pensant qu'il s'agissait de ces messieurs.

Qu'après l'acceptation de la demande d'amitié, les personnes sur les profils ont commencé à échanger des messages écrits en portugais, à travers le Messenger, et pendant la conversation, il leur promet une offre d'emploi aux Nations Unies (UN), en tant que diplomate représentant le Cap Vert, dont le salaire serait d'environ cinq mille dollars par mois (environ 500.000$00 mille escudos cap-verdiens) en tenant compte que le salaire minimum en CV est de 13.000$00 mille escudos (130 Dollars USD).

Après avoir fait cette promesse de travail et l'avoir acceptée, la personne aux profils leur fournit un contact qu'elle prétend être un fonctionnaire de l'ONU, avec lequel les victimes doivent commencer à parler pour traiter des questions liées à l'embauche pour le poste.

En général, ce contact est un numéro dans WhatsApp, et les victimes commencent à parler à la personne qui, dans tous les cas signalés, a déclaré qu'il s'agissait d'une voix d'homme. La personne leur demande d'envoyer des documents, tels qu'une copie du passeport, du curriculum vitae, du casier judiciaire, et de l'argent par virement pour payer les frais de traitement des documents (contrats de travail, badge d'identification en tant qu'employé de l'ONU, etc.)

Les victimes envoient les sommes demandées via Western Union ou Money Gram, des montants d'environ 100 000 escudos (1000 euros), mais quelques jours plus tard, cette personne les recontacte pour leur demander plus d'argent pour le processus d'embauche et, pour plus de crédibilité, ils envoient un contrat de travail qui doit être signé et envoyé par courrier électronique. Une fois le contrat signé et envoyé, elle demande à nouveau des montants supplémentaires, avec d'autres justifications. Cependant, si la victime s'avère incapable de payer, ils menacent d'annuler le contrat.

Une fois que les victimes sont désespérées, lorsqu'elles ne sont plus en mesure de payer, elles vont voir le ministre en personne ou le font par l'intermédiaire de tiers connus du ministre et c'est ainsi qu'on leur explique qu'elles sont entrées dans un système où elles ont été trompées par des cybercriminels, et donc que les profils n'appartiennent pas aux ministres. En d'autres termes, ils sont faux.

En ce qui concerne les faits exposés ci-dessus, dans lesquels il y a sept (07) victimes, les cybercriminels ont eu un revenu d'un montant total de 3.387.730$00 ECV, correspondant à (USD 31.709,2). Cependant, tout l'argent a été envoyé via Western Union, pour le Bénin, plus précisément Cotonou.

Source : Cabo Verde

Cas 6 : Escroquerie à la proposition commerciale et fraude à l'avance de frais

Le 3 décembre 2018, le CENTIF-TOGO a reçu une déclaration de soupçon de la part d'une institution financière A suite à plusieurs transferts de fonds reçus de l'étranger par Monsieur KM. A l'ouverture du compte, il a déclaré être le gérant de la société ES dont l'activité est l'import-export de chaussures et de sacs. Pour une société dont la vocation est l'import-export, des fonds devraient normalement être envoyés du Togo vers l'étranger pour l'achat de marchandises, mais non seulement le compte n'a jamais été transféré à l'étranger, mais il a plutôt fonctionné comme un compte à rebond, où les fonds des transferts reçus sont immédiatement retirés, laissant le compte en sommeil jusqu'à ce qu'un nouveau transfert soit reçu. Cette situation s'inscrit dans le cas atypique d'une cyber-fraude de type 419. Les investigations de la CENTIF ont révélé qu'il dispose d'un autre compte au niveau d'une institution financière B et dont le fonctionnement est identique à celui du compte de l'institution A. Le 18 juin 2021, la CENTIF-TG a reçu un partage d'informations de son homologue au Japon concernant Monsieur KM, pour des faits de tentative d'escroquerie à travers un transfert frauduleux. En effet, le 25 décembre 2020, un ressortissant japonais Monsieur JJ se présente aux guichets d'une banque de son pays et insiste sur le fait qu'il dispose de 3 300 000 USD soit environ 1 980 000 000 FCFA sur son compte bancaire au Togo. Ce compte s'avère être le compte B de M KM. M. JJ demande alors à sa banque de transférer 400 USD sur ledit compte afin d'effectuer les formalités pour récupérer les 1.980.000.000 FCFA qui s'y trouvent. L'institution financière japonaise refuse d'exécuter l'ordre de transfert car elle a des doutes sur le motif du transfert et dépose une déclaration de soupçon auprès de la cellule de renseignement financier du Japon qui, à son tour, signale l'affaire à la CENTIF TOGO. Cependant, la victime s'est laissée extorquer entre 2015 et 2021, et a effectué 41 transferts de fonds reçus, soit au moins 37.598.670 FCFA.

Source : Togo

Cas 7 : Escroquerie à la romance / à l'or et fraude à l'avance de frais

Étude de cas 2

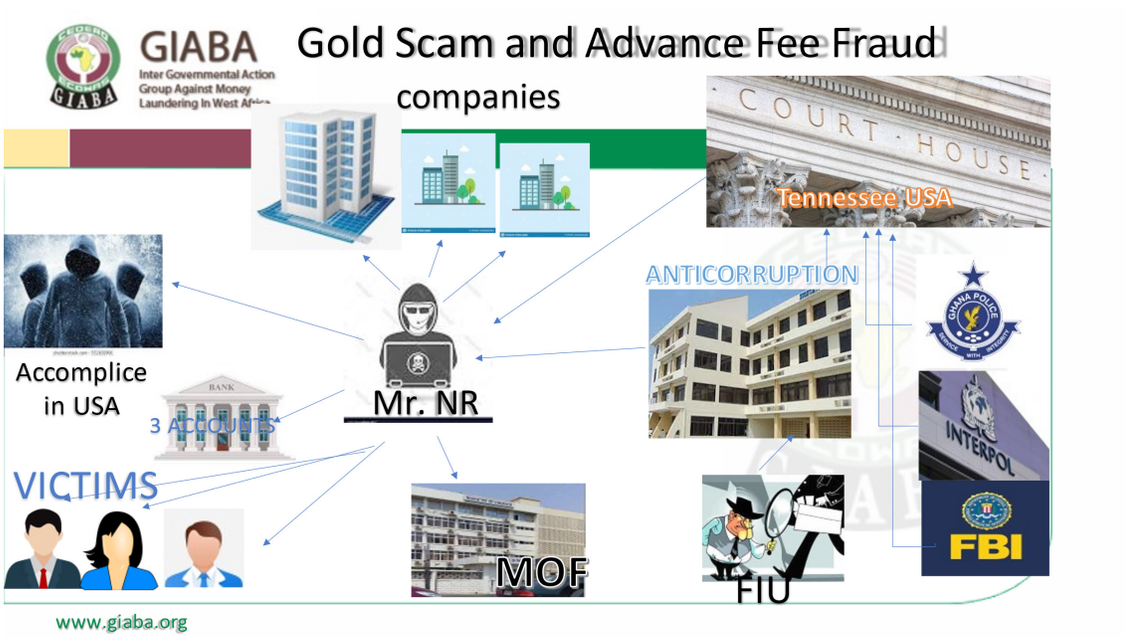
Le FIC a transmis à l'EOCO un renseignement sur les activités d'un ressortissant nigérian résidant au Ghana, qui possédait et exploitait une société dont les activités étaient de nature maritime, de soutage, de transport maritime et de construction. Il a attiré l'attention du Centre de renseignement financier (FIC) lorsqu'il a reçu des fonds en provenance des États-Unis. Lorsqu'il a été interrogé sur ces entrées de fonds, il a déclaré qu'il était sur le point de créer une banque et qu'il était en train d'obtenir l'approbation de la Banque du Ghana. En août 2016, il a reçu des fonds supplémentaires d'un montant total de 330 749,47 USD provenant de trois sources, une société aux États-Unis et deux citoyens américains. Son compte bancaire a été immédiatement gelé par l'EOCO et une enquête a été ouverte. Au cours de l'enquête, il a été établi qu'il s'était présenté sous un faux jour à certaines des victimes qu'il avait rencontrées sur le site de rencontre www.match.com comme un homme blanc travaillant sur des projets au Ghana, avec de faux noms d'emprunt. Il s'est également présenté comme un trafiquant d'or opérant sous le nom de deux fausses sociétés qui auraient possédé de l'or d'une valeur de 8 millions de dollars américains. Il a également présenté de faux documents censés émaner du ministère des finances pour prouver que l'or qu'il prétendait détenir se trouvait au ministère.

En août 2017, alors que l'enquête était en cours au Ghana, un grand jury fédéral du tribunal de district des États-Unis pour le district occidental du Tennessee a inculpé le suspect et d'autres personnes pour conspiration en vue de commettre une fraude électronique, conspiration en vue de commettre un blanchiment de capitaux, conspiration en vue de commettre une fraude informatique et un vol d'identité aggravé. La cour fédérale a indiqué que le suspect, en collaboration avec d'autres complices aux États-Unis, a déployé des techniques d'anonymisation sophistiquées, y compris l'utilisation d'adresses électroniques usurpées et de réseaux privés virtuels, les complices ont identifié des transactions financières importantes, ont initié une correspondance électronique frauduleuse avec les parties commerciales concernées et ont ensuite redirigé les fonds de clôture. Les victimes ont été identifiées comme étant originaires des États-Unis, d'Australie, du Royaume-Uni et de Finlande.

Il a été extradé vers les États-Unis en décembre 2019 et a été condamné à 3,5 ans de prison le 16 juin 2021. L'enquête a bénéficié de la collaboration du FIC, des services de police du Ghana, d'Interpol et du FBI à tous les niveaux, ce qui a permis de mener à bien l'enquête et les poursuites. Aucun lien avec le financement du terrorisme n'a été identifié. En juin 2022, l'EOCO a entamé une action en justice pour rapatrier aux États-Unis les produits du crime qui ont été gelés sur les différents comptes bancaires.

Source : Ghana

Titre : version française *(à envoyer)*



Méthodes et techniques

- Utiliser un site de rencontre populaire en utilisant une fausse identité
- Établissement d›une relation en ligne ou à distance et d›une relation de confiance pour attirer les victimes
- Recours à des professionnels tiers, notamment des personnes morales
- L'utilisation des commerces de façade

Drapeaux rouges et indicateurs

- Transactions financières inhabituelles
- Incohérences dans les déclarations lors des interrogatoires des forces de l'ordre
- Fonds reçus sur un compte dont le nom du bénéficiaire est différent de celui du compte

Cas 8 : Escroquerie aux contrats commerciaux (import/export) et fraude aux avances de frais

XZ, résidant à Niamey, a reçu un appel téléphonique (GSM) en provenance d'un numéro dont l'indicatif est la France. Son interlocuteur au téléphone, qui se présente comme GMN, a recueilli suffisamment d'informations spécifiques sur lui pour que XZ croie que GMN le connaît depuis longtemps. GMN parvient à établir et à gagner la confiance de XZ par le biais d'une ingénierie sociale bien huilée. GMN propose à XZ de lui livrer une des sèves de moringa. GMN explique à XZ qu'il avait une telle relation d'affaires avec une personnalité connue mais décédée. XZ est donc choisi pour remplacer celle-ci, lui explique GMN, en précisant la quantité souhaitée. GMN explique à XZ que la sève de moringa est un produit très populaire qu'il recherche pour le compte d'un médecin travaillant pour un laboratoire basé en France chez Carrefour KYC.

GMN communique à XZ le nom de Kaboré Elh Moussa, domicilié à Ouagadougou, ainsi que le numéro de téléphone de BBP auprès duquel Kaboré et GMN prétendent s'être approvisionnés en sève de moringa par le passé. XZ est informé qu'il doit contacter BBP pour lui demander s'il a encore de la sève de moringa en quantité et en qualité et en même temps s'enquérir du prix.

Après que XZ et BBP se soient mis d'accord sur la quantité disponible ainsi que sur le prix, BBP propose à XZ de recevoir d'abord un premier échantillon. Cet échantillon est livré directement à Niamey par une personne présentée comme le fils de BBP qui perçoit personnellement les frais relatifs au prix de l'échantillon. L'échantillon est soumis à l'expertise d'AC, un Européen dont le numéro de téléphone a été communiqué à XZ par Kaboré Elh Moussa. Une fois la qualité confirmée par AC, XZ et BBP se sont mis d'accord sur les conditions de livraison (coûts, modes de transport, etc.) pour l'ensemble de la commande. Pour ce faire, plusieurs frais supplémentaires sont demandés à XZ en fonction de la nature des marchandises. Il s'agit des frais d'emballage, de conditionnement, phytosanitaires, et des formalités administratives y compris douanières.

Après tous ces frais, y compris le prix d'achat de la commande groupée et d'autres frais supplémentaires, XZ, qui attendait anxieusement que la sève de Moringa lui soit livrée, a tenté en vain de joindre GMN, Kaboré, BBP, AC et le fils présumé de BBP. Tous avaient éteint leur téléphone portable.

Mécanisme, instrument et technique de la CB identifiés dans l'affaire

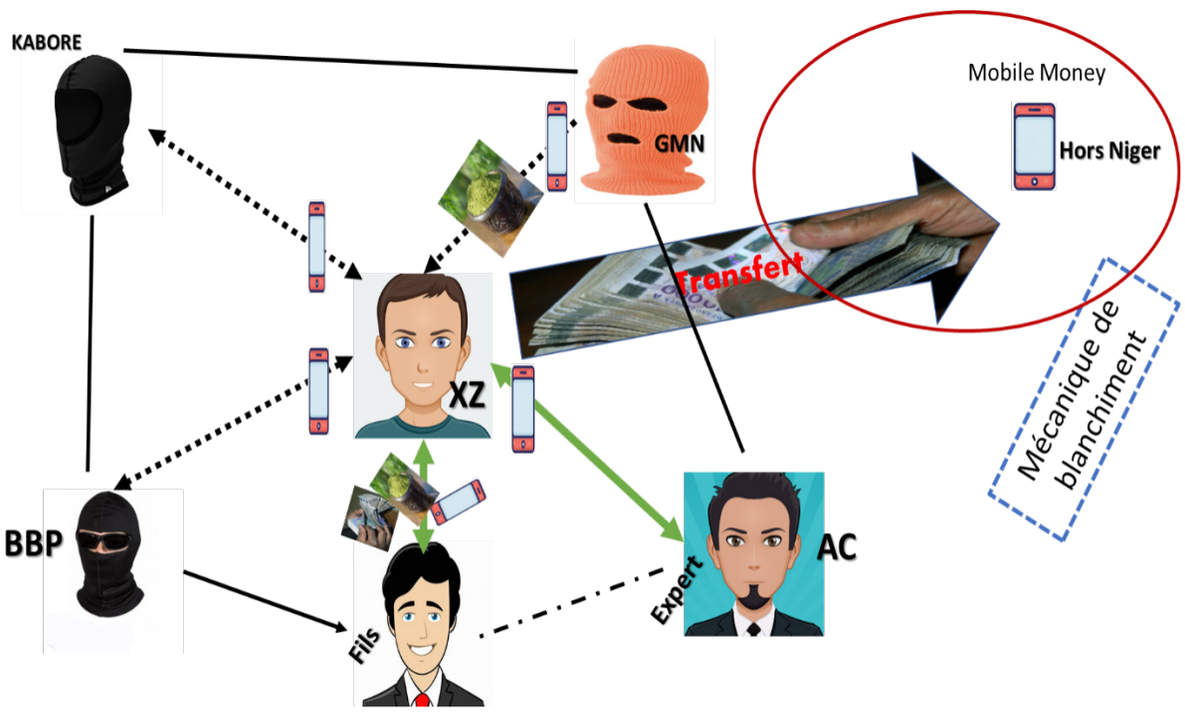
Depuis la négociation et la remise des fonds, XZ n'a rencontré physiquement que deux (02) personnes : le fils présumé de BBP qui lui remet l'échantillon pour analyse et l'expert AC chargé d'analyser ledit échantillon. Toutes les manœuvres frauduleuses qui ont enlevé à XZ la volonté de remettre ses fonds n'ont été possibles que grâce à une méthode bien connue en cybercriminalité : l'ingénierie sociale via les TIC.

L'infraction principale de fraude par communication électronique a généré des fonds qui ont été placés à l'extérieur d'un mécanisme, à savoir l'argent mobile, et qui ont entamé un processus de compensation (transfert vers l'extérieur) par le même mécanisme (application d'argent mobile).

Lors de leur arrestation, les suspects ont été trouvés en possession d'objets compromettants tels que des téléphones portables, des cartes SIM, des reçus de transfert de fonds, de faux documents d'identité utilisés pour les retraits, ainsi que des sacs contenant des graines noires.

Les suspects ont été renvoyés au parquet pour escroquerie par un moyen de communication électronique sans avoir été instruits par l'OPJ sur le fondement du BCFT.

Source : Niger



Cas 9 : Escroquerie aux services de fret du commerce international et fraude à l'avance de frais

L'affaire a commencé au début de l'année 2012, lorsque l'accusé a été repéré par la FIC pour des entrées illicites présumées sur ses comptes bancaires. L'accusé est entré en hibernation lorsque son compte a été gelé et a refait surface en 2016 sous de multiples identités. L'accusé a utilisé trois passeports différents portant des noms différents pour ouvrir et gérer sept comptes dans différentes succursales de la banque «A». L'accusé possédait également des comptes auprès de quatre autres banques, qu'il avait ouverts en utilisant de faux documents, tels que de faux passeports et de fausses cartes d'électeur. L'accusé s'est ensuite frauduleusement présenté en ligne à ses victimes comme un homme d'affaires sous les noms de George Hanson et Daniel Brown, qui proposait des services de transport international de marchandises dans le monde entier. Le système est structuré de telle sorte que ses services sont recommandés par de prétendus clients (ses co-conspirateurs) de victimes (clients potentiels), principalement des États-Unis, du Royaume-Uni et d'autres pays comme l'Australie, qui finissent par effectuer des paiements anticipés pour ses services. Il a reçu des victimes plus de 20 envois de fonds d'un montant total de 351 000 USD et 40 000 GBP supplémentaires sur ses multiples comptes.

L'enquête a établi que l'accusé avait utilisé une partie du produit de son crime pour se procurer une maison au Ghana. Il a dépensé une partie de l'argent et disposait d'un solde de 10 000 GBP sur son compte, qui a été gelé pendant l'enquête. Il a été inculpé, entre autres, de blanchiment de capitaux, d'escroquerie par faux semblants, de fraude fiscale, d'usurpation d'identité et de falsification de documents. Au tribunal, bien que l'accusé ait plaidé non coupable de tous les chefs d'accusation, la cour l'a reconnu coupable et l'a condamné à deux ans d'emprisonnement et à une amende de trois mille unités de pénalité, ou, à défaut, à trois ans supplémentaires, pour les chefs d'accusation de falsification,

après que l'accusation a prouvé son bien-fondé. Pour le blanchiment de capitaux, l'accusé a été reconnu coupable et condamné à une peine de deux ans et à une amende de quatre mille unités de pénalité ou, à défaut, à quatre ans de travaux forcés. Le tribunal a également ordonné la confiscation de tous les fonds de l'accusé, et les biens fonciers, y compris la maison acquise, ont été confisqués au profit de l'État, en plus des 10 000 GBP restant sur son compte bancaire.

Source : Ghana

Cas 10 : Escroquerie à la romance / à l'héritage et fraude à l'avance de frais

Étude de cas 1 (cas d›escroquerie au romantisme et à l›héritage)

L'accusé a été arrêté pour avoir participé à un vaste projet d'escroquerie d'un montant de 700 000 USD à l'encontre d'un résident de New York, aux États-Unis. L'accusé (un homme), utilisant une fausse identité féminine (Mlle X), a entamé une relation amoureuse en ligne avec la victime. L'accusé s'est assuré les services d'une actrice pornographique populaire, Mlle Y, résidant aux États-Unis, qui s'est présentée sous la fausse identité de Mlle X pour que la relation ait l'air réelle. L'actrice pornographique a convaincu la victime de l'existence d'un héritage en or qu'elle possédait au Ghana et tous deux se sont rendus dans ce pays. Au Ghana, elles ont rencontré un chauffeur de taxi appelé «Z», qui s'est avéré être l'accusé et le cerveau de l'opération. Mlle X a présenté à la victime de faux documents montrant qu'elle avait hérité d'une mine d'or nommée Company A et qu'elle souhaitait la transférer à son nom et à celui de la victime. En conséquence, la victime a transféré un montant total de 428 865 USD sur les comptes bancaires d'une société qui s'est avérée appartenir à l'accusé et un autre montant de 349 993 USD à une société immobilière sur les instructions de l'accusé, à titre de paiement pour de l'or. Au cours de l'enquête, la société immobilière qui a reçu 349 993 USD a affirmé que l'accusé l'avait chargée de concevoir et de construire un manoir pour lui dans un quartier privilégié d'Accra, au Ghana. Dans le cadre de la même entreprise frauduleuse, l'accusé a construit et meublé un manoir de trois chambres pour son père, et a également acquis un véhicule privé - Hyundai Tucson.

L'accusé a été inculpé de blanchiment de capitaux, d'usurpation d'identité, d'escroquerie sous de faux prétextes et de falsification de documents et a été traduit devant la High Court - Financial Crime Division. En août 2020, alors que les poursuites étaient en cours, la Cour a été informée du décès de l'accusé. Le tribunal a ordonné le gel des avoirs de l'accusé et un administrateur général a été nommé pour superviser la succession de l'accusé, conformément à la loi de 1961 sur l'administration des successions, à la demande de l'EOCO. Le père de l'accusé a intenté une action en vue de rejeter la requête contre l'accusé, au motif que la requête initiale avait été déposée contre l'accusé, qui était décédé, et qu'elle était donc incompétente et devait être rejetée. Toutefois, l'affaire a été examinée à la lumière de l'article 50 de la loi sur la criminalité économique et organisée, qui autorise la Cour à confisquer des biens entachés si la personne dont les biens ont été saisis décède ou se soustrait à la justice ; la Cour a donc donné raison à l'EOCO.

Source : Ghana

Cas 11 : Escroquerie au romantisme et fraude à l'avance de frais

La NFIU a reçu une transaction suspecte déposée par une entité déclarante impliquant de multiples transactions à haut volume à hauteur de 4 981 206,32 NGN. Les fonds ont été reçus par un certain M. X entre le 2 juillet et le 17 août 2020, en 10 transactions via Western Union Money Transfer. Les transactions ont été envoyées depuis le Canada par Mme Y, sans justification ni preuve d'un lien de parenté. Le volume élevé des transactions est un signal d'alarme, tout comme le fractionnement des transactions pour éviter le seuil limite. Le lieu de résidence et l'âge du destinataire éveillent également les soupçons d'une escroquerie à la romance. L'affaire a été transmise aux services répressifs compétents et fait actuellement l'objet d'une enquête pour escroquerie à la romance, fraude à l'avance de frais et blanchiment de capitaux.

Source : Nigeria

Cas 12 : Escroquerie au romantisme / Faux-semblants et fraude à l'avance de frais

Cette affaire a été signalée à la police en 2022. Les victimes ont déclaré que le ou les suspects, dont on pense qu'ils se trouvent au Nigeria, ont ouvert plusieurs comptes en utilisant de faux noms et des photos de belles dames blanches, puis ont attiré des hommes dans une relation en ligne. Au cours de ce processus, ils font croire à leurs victimes qu'elles doivent préparer un certain document appelé «affidavit de confiance pour une relation à distance». Dans leur quête pour obtenir ce document, les victimes sont dirigées vers un prétendu avocat qui ferait partie du syndicat criminel et qui leur extorque de l'argent au nom de la fourniture de ce document.

L'enquête a établi que les suspects susmentionnés ont réussi à escroquer leurs victimes en leur remettant une somme de 587 700,00 (cinq cent quatre-vingt-sept mille sept cents dalasis) (10 494,6 USD) qui a été versée sur des comptes bancaires au Nigeria.

Une lettre a été envoyée à Interpol Nigeria afin de localiser le suspect et de récupérer éventuellement l'argent obtenu illégalement auprès de ses victimes, mais aucune réponse n'a été reçue jusqu'à présent.

Source : Gambie

Cas 13 : Traite des êtres humains, enlèvement, sextorsion et extorsion de fonds

Dans une affaire traitée par le DSC, un chef de réseau cybercriminel, profitant de la situation de vie difficile de deux jeunes Nigérianes, les a emmenées au Sénégal, sous prétexte qu'il était en mesure de leur trouver un emploi.

Une fois à Dakar, il leur a confisqué leurs documents de voyage, leur a fait passer des tests de dépistage du VIH et du sida, puis les a contraintes à une forme d'esclavage sexuel sous peine de mort.

Il photographiait les filles nues et utilisait les images comme appât pour ses victimes dans le cadre de ses activités cybercriminelles.

Il les forçait également à coucher avec des Européens qu'il invitait au Sénégal, kidnappait et libérait après que leurs parents aient payé une rançon.

Son mode opératoire consistait à contacter ses proies par Messenger, en se présentant avec des profils de jeunes filles. Ensuite, il les utilisait pour communiquer via WhatsApp avec les victimes afin de les rassurer. C'est sur la base de ces manœuvres qu'ils ont réussi à attirer cinq (05) ressortissants européens, qui ont été séquestrés et libérés après paiement de rançons.

Ce réseau très structuré disposait d'antennes dans la sous-région où certains membres du groupe étaient chargés d'encaisser les fonds issus de leurs activités qu'ils transféraient via des systèmes de transfert électronique.

Afin de récupérer l'argent transféré à la suite du chantage, le chef du gang a coopéré avec certains responsables de l'agence de transfert d'argent qui ont remis les fonds en dépit de la procédure normale.

Source : Sénégal

Cas 14 : Fraude, chantage, extorsion et blanchiment de capitaux

En 2022, l'apprenti chauffeur MSD de la ville de Koundara en Guinée, de retour dans sa ville natale, après un long séjour dans un pays voisin de la Guinée, a décidé de se lancer dans des activités cybercriminelles pour subvenir à ses besoins. Il a créé un compte Facebook et s'est fait passer pour une femme nommée AB pour les besoins de la cause, il a téléchargé plusieurs photos d'une femme au physique attrayant à partir d'un compte Instagram et a envoyé des invitations à plusieurs hommes d'âge mûr qui ont répondu auxdites demandes.

C'est ainsi qu'ont débuté entre MSD agissant sous l'identité d'AB et ses victimes, des conversations intimes au cours desquelles ils ont proposé à ce dernier d'entretenir des relations charnelles par mode d'appel vidéo et ont réussi à filmer ses victimes, qu'il a ensuite fait chanter en les menaçant de payer entre 5 000 et 10 000 dollars US par mois sous peine de voir leurs nudités exposées sur les réseaux de médias sociaux.

Les victimes étant généralement des hommes respectables, elles lui versaient les sommes demandées. Les différents montants récoltés ont été utilisés par le cybercriminel pour mettre en place plusieurs projets : l'achat d'un mini-bus pour les transports publics, d'une voiture pour ses déplacements personnels et enfin la construction d'un vidéo-club et d'un bar. Ces montants sont estimés à plus de 50 000 dollars américains.

Après avoir reçu plusieurs plaintes, la cellule de lutte contre la cybercriminalité de la direction centrale de la police judiciaire a entrepris sans hésiter des investigations numériques qui ont conduit à l'arrestation du suspect, qui a reconnu sans ambages les faits qui lui sont reprochés et a demandé l'indulgence des autorités chargées de l'application de la loi. Au terme des investigations, le prévenu a été déféré au parquet de Kaloum qui a demandé l'ouverture d'une information judiciaire pour les délits d'escroquerie, de chantage et d'extorsion de fonds, le tout par le biais d'un système informatique et de blanchiment de capitaux.

À ce jour, la procédure a abouti à un procès et le délinquant a été condamné à cinq ans d›emprisonnement et à une amende de 500 000 000 GNF par le tribunal pénal de Kaloum, et ses biens ont été confisqués conformément aux lois sur la lutte contre le blanchiment de capitaux et le financement du terrorisme et sur la cybersécurité. MSD est détenu à la prison centrale de Conakry.

Source : Guinée

Cas 15 : Escroquerie aux contrats commerciaux (import/export) et fraude aux avances de frais

En juillet 2022, un ressortissant ukrainien a déposé une plainte auprès de l'EOCO, alléguant qu'il avait été escroqué de 6,5 millions de dollars. M. X, un ressortissant nigérian résidant au Ghana, s'est engagé à fournir à M. F, un ressortissant ukrainien, des poteaux en bois de teck en provenance du Ghana en 2018. Des photos de poteaux de teck prétendument emballés dans un entrepôt sous douane ainsi que des documents d'expédition ont été envoyés à l'Ukrainien comme preuve que les marchandises étaient sur le point d'être expédiées. L'Ukrainien a versé 6,5 millions de dollars par virement bancaire en paiement des produits. L'Ukrainien a ensuite chargé deux avocats ghanéens, V et K, de superviser les transactions. V et K auraient découvert que la transaction était fictive, mais auraient incité l'Ukrainien à effectuer les paiements. L'avocat V a confirmé avoir reçu des honoraires d'avocat de l'Ukrainien ainsi que 600 000 GHS de M. X. M. X, V et K ont été arrêtés et inculpés de blanchiment de capitaux, de conspiration frauduleuse et d'escroquerie sous de faux prétextes. Ils sont actuellement détenus par l'EOCO.

Source : Ghana

Cas 16 : Fraude, chantage, extorsion et blanchiment de capitaux

En décembre 2022, AOK, un entrepreneur résidant au quartier Sonfonia, dans la commune urbaine de Ratoma/Conakry, reçoit un appel téléphonique d'un inconnu qui lui dit à l'autre bout du fil qu'il est un grand devin. Ainsi, l'inconnu l'a décrit et lui a donné des informations précises sur sa famille, ses activités, sa vie privée et lui a ensuite révélé qu'il courrait un grand danger s'il ne faisait pas de grands sacrifices pour éviter ce qui allait lui arriver. Les sacrifices proposés étaient les suivants 10 bœufs, 2 chameaux, 5 moutons à sacrifier et une somme de 25 millions de francs (2 500 USD) à utiliser pour acheter d'autres objets à considérer pour des travaux occultes.

L'inconnu lui a conseillé de ne pas expliquer cette situation à qui que ce soit, même à sa femme, au risque d'être atteint de folie. Il lui conseille d'agir vite car le temps presse. Étonné, bouleversé et effrayé par ces propos inattendus et craignant pour sa vie, il réunit la somme de 25 millions ainsi que la valeur des animaux mentionnés ci-dessus, le tout faisant 110 000 000 FG (11 000 USD). Il demande à l'inconnu, qui n'est autre qu'IKK, de lui indiquer comment il peut lui faire parvenir cette somme dans les plus brefs délais.

Le suspect lui a ainsi donné 5 numéros de téléphone avec des comptes d'argent mobile sur lesquels il lui a demandé de fractionner le dépôt de la somme, à raison de 22 000 000 FG par compte. Après avoir effectué le paiement, le suspect lui a demandé d'aller chercher de l'eau de mer à minuit, de verser cette eau dans une jarre encore neuve et inutilisée, d'ajouter du lait de vache frais à l'eau et de se laver avec le mélange le lendemain matin après avoir observé un jeûne tout au long du processus. Il lui a demandé de rester à l'écart pendant 3 semaines, après le rituel, sans toucher une femme.

Un mois après avoir effectué le rituel, AOK a reçu un autre appel téléphonique du suspect qui l'informait encore d'un autre rêve, dans lequel ses enfants étaient entourés d'une meute de chiens noirs qui menaçaient de les dévorer et qu'il fallait rapidement conjurer le sort pour éviter que les enfants ne soient victimes de sorcellerie. Comme pour la première fois, il indique des animaux à sacrifier et une somme de 26 millions (2 600 USD) à payer. Effrayé par cette nouvelle révélation, AOK a refusé d'obtempérer et a affirmé qu'il n'avait plus les moyens de faire face à la nouvelle exigence du devin. Le suspect, après avoir entendu cela, a commencé à menacer AOK par d'autres chiffres et parfois par des intermédiaires.

Inquiet de la situation, AOK a décidé d'informer sa femme, allant à l'encontre de l'avertissement du soi-disant devin. Celle-ci a informé son frère, officier de police judiciaire, qui a conseillé à son beau-frère de déposer immédiatement une plainte auprès de l'unité de lutte contre la cybercriminalité de la direction centrale de la police judiciaire.

Dès réception de la plainte d'AOK, l'Unité de Cybercriminalité de la Direction Centrale de la Police Judiciaire a, sans hésitation, immédiatement entamé des investigations en étudiant l'identification numérique des utilisateurs des différents numéros utilisés pour échanger avec lui. Une réquisition a donc été adressée à l'ARPT aux fins de communiquer l'historique des appels entrants et sortants des numéros suspects ainsi que la géolocalisation des utilisateurs. Les résultats des investigations numériques ont indiqué que les appels téléphoniques provenaient de Labé, plus précisément du centre de détention. Une mission a été envoyée, sous la direction du procureur de la République, pour réprimander les prévenus opérant à partir de ce centre de détention. Après une demi-journée de perquisitions dans les différentes cellules, 22 téléphones ont été saisis. Après d'intenses investigations, les détenus ont finalement collaboré et dénoncé leurs codétenus impliqués dans l'escroquerie, dont certains avaient déjà retiré les puces des téléphones.

Interrogé par les enquêteurs, IKK, l'auteur principal, mis devant le fait accompli, a reconnu les faits de fraude et d'extorsion par le biais d'un système informatique dont AOK a été victime, et a dénoncé ses complices qui ne sont autres que ELMO, qui jouait le rôle de vendeur de bétail, ELGA qui était chargé de se rendre dans les différents kiosques de mobile money afin d'y retirer les différents montants. Il a également dénoncé FORCE, le gardien de prison qui a non seulement facilité l'acquisition des téléphones portables, mais a également servi d'intermédiaire pour collecter de l'argent au nom du suspect à l'extérieur de la maison de détention, en échange de pots-de-vin. IKK a également dénoncé deux éleveurs et un boucher qui lui ont permis de blanchir le produit de ses actes cybercriminels.

Au terme des investigations, le prévenu et ses complices ont été déférés au parquet de Labé qui a requis l'ouverture d'une information judiciaire pour les délits d'escroquerie, de chantage et d'extorsion de fonds, le tout par le biais d'un système informatique et de blanchiment de capitaux. A ce jour, les prévenus ont tous été renvoyés devant la juridiction de jugement, au tribunal correctionnel de Labé.

Source : Guinée

Cas 17 : Fraude, usurpation d'identité, fraude à l'avance de frais et blanchiment de capitaux

L'EOCO a reçu un rapport de renseignement du Centre de renseignement financier (FIC) en janvier 2017 selon lequel le premier accusé (A1), un ressortissant étranger détenteur d'un passeport américain, a reçu divers envois de fonds d'un montant total de 1 551 953,55 GHS (309 000 USD) sur son compte auprès d'une banque ghanéenne. Il s'est avéré que A1 a ouvert et géré le compte bancaire avec une fausse carte d'identité et d'autres documents falsifiés qui indiquaient faussement qu'il était ambassadeur des Nations unies. Avant d'ouvrir son compte bancaire, A1 avait également reçu plusieurs envois de fonds via des transferts MoneyGram et Western Union.

Lorsque les fonds de A1 ont été retenus, en raison de leur nature suspecte, pour une enquête plus approfondie, le deuxième accusé (A2), utilisant de faux documents au nom d'éminents ministres ghanéens, s'est présenté comme un avocat des Nations unies au Ghana et a tenté d'obtenir le déblocage des fonds en faveur de A1. A2 a prétendu que les fonds provenaient de Singapour et devaient être remis à A1 pour l'aider à payer des institutions telles que le ministère des finances et la banque du Ghana pour certains projets présumés des Nations unies exécutés au Ghana. A1 a prétendu qu'il était au Ghana pour entreprendre un projet pour les réfugiés et qu'il était ambassadeur élu de l'ONU pour les réfugiés depuis 2015. Les enquêtes ont cependant révélé que A1 n'était pas un représentant de l'ONU et qu'il n'avait jamais entrepris de projet pour l'ONU. Les enquêtes ont montré que ces transferts de fonds étaient le produit d'un crime, dont A1 et A2 ont cherché à dissimuler la source et l'objectif.

Le troisième accusé (A3), alors directeur de l'agence de la banque où A1 avait ouvert son compte, a délibérément violé les procédures d'ouverture de compte et les règles KYC pour permettre à A1 de recevoir et de dissimuler les fonds viciés. La banque, après avoir détecté les violations, a déposé une déclaration de transaction suspecte (DTS) auprès de la FIC, qui a également transmis l'affaire à l'EOCO pour enquête. L'enquête n'a pas été en mesure d'interroger les expéditeurs de fonds pour confirmer que les transferts de fonds étaient frauduleux, et aucune plainte pour vol ou fraude n'a été déposée contre les accusés par les expéditeurs de fonds. Toutes les tentatives faites par l'enquête, y compris le recours à l'entraide judiciaire, se sont révélées vaines. Néanmoins, les suspects ont été inculpés de blanchiment de capitaux, de falsification de documents, d'usurpation d'identité, d'escroquerie sous de faux prétextes, de complicité de falsification, d'aide et de complicité de blanchiment de capitaux, conformément aux sections 1 et 2 de la loi de 2008 sur le blanchiment de capitaux (loi 749), de désobéissance à une obligation conformément à la loi de 2000 sur l'immigration (loi 573) et d'évasion fiscale conformément à la section 149 de la loi de 2000 sur le revenu interne (loi 592). Les poursuites sont toujours en cours.

Source : Ghana

Cas 18 : Escroquerie au commerce en ligne, usurpation d'identité et fraude à l'avance de frais

En octobre 2021, Mme ANDA, de Bafata, a contacté la police au sujet d'une escroquerie en ligne présumée perpétrée par un suspect originaire d'un pays voisin. Le suspect vendait prétendument des cheveux artificiels présentés sur sa page Facebook sous le nom de Tafa Cabélo. Le suspect contacte ses victimes dès qu'elles expriment un intérêt pour l'achat de ces cheveux. Le suspect Tafa a dit à Mme ANDA que les cheveux qu'il voulait coûtaient 190 000 FCFA (300 USD), mais qu'elle devait faire un paiement anticipé via mobile money de 50 000 FCFA (95 USD) pour passer commande. Comme Mme ANDA était intéressée, elle a envoyé l'argent. N'ayant pas eu de nouvelles du suspect pendant des semaines, elle l'a appelé pour s'enquérir de la commande, ce à quoi le suspect a répondu que sa cargaison était sur le point d'arriver. Au bout d'un certain temps, le suspect l'a appelée, lui demandant d'avancer 90 000 FCFA supplémentaires pour qu'il puisse expédier sa commande à la frontière. Cette dernière demande éveille les soupçons de Mme ANDA qui n'en fait pas part au suspect mais alerte la police des frontières de Bissau. En accord avec la police, elle invente une histoire qui implique son frère NANO, résidant à Pefine. NANO a alors appelé le suspect comme convenu par Mme ANDA, confirmant qu'il allait livrer la somme demandée à la frontière. La police les a ensuite guidées sur la manière de procéder en termes de communication avec le suspect, alors qu'elles procédaient à l'arrestation du suspect à côté de la station-service ELTON située à Bandim.

En outre, l'analyse du téléphone du suspect a révélé qu'il trompait depuis longtemps des femmes en leur faisant miroiter la vente de cheveux, par le biais de son compte Facebook et, par conséquent, de Messenger, et qu'il avait créé à cette fin deux comptes sur les réseaux partenaires avec les noms suivants : FALL TÈRANGA EL TIFRÈ et TAFA CABÉLO, afin d'attirer ses victimes.

Le suspect a été remis au ministère public pour la poursuite de l'enquête et des poursuites.

Source : Guinée Bissau

Cas 19 : Escroquerie aux contrats commerciaux (import/export) et fraude à l'avance de frais

En 2019, l'agence chargée de la lutte contre la cybercriminalité a reçu des plaintes concernant certains individus impliqués dans une affaire d'escroquerie aux contrats d'exportation. Cette bande organisée de l'intérieur et d'un pays voisin a contacté par téléphone la victime GSS en prétendant l'avoir rencontré et connu il y a longtemps. Après avoir convaincu le GSS qu'il s'agissait d'une ancienne connaissance et prétendument de médecins, ils lui ont proposé un contrat d'exportation portant sur la fourniture de racines d'»Artemisia». Ils ont ensuite persuadé GSS de la nécessité d'effectuer des transferts pour couvrir les coûts d'exportation (achat du produit, stockage, transport, emballage, formalités douanières et autres), et ont réussi à lui extorquer frauduleusement de l'argent. GSS a transféré les fonds qui ont été retirés par des moyens électroniques (Mobile money, Western Union, etc.). L'enquête a conduit à l'arrestation de SKS et de 47 autres suspects, dont un ressortissant d'un pays voisin, identifié comme un membre actif du gang.

Le procureur spécial de la CRIET a été saisi de l'affaire et, après avoir déclaré l'accusé coupable, le tribunal a condamné SKS à sept (7) ans d'emprisonnement avec une amende d'un million de FCFA (1 522 USD) et a ordonné le remboursement d'un million sept cent trente-six mille cent FCFA (2 642 USD) à GSS.

Source : Bénin

Cas 20 : Escroquerie au romantisme / Faux-semblants et fraude à l'avance de frais

En 2019, l'agence principale chargée de la lutte contre la cybercriminalité a reçu un renseignement sur une bande organisée de cybercriminels résidant à Cocotomey dans l'arrondissement de Gbodjè. Après enquête et découverte de la localisation des membres du gang, LCD, KRH et DR ont été arrêtés en janvier 2020. LCD a révélé utiliser le profil d'une femme pour attirer ses victimes dans l'arnaque à la romance, tandis que KRH utilise sur son profil la photo d'une femme nécessiteuse à la recherche d'une aide financière. Quant à DR, il propose sur Internet des contrats fictifs pour obtenir un prêt. KE, un complice chargé d'effectuer les retraits des fonds générés par ces activités cybercriminelles, a également été arrêté. Déférés au parquet spécial de la CRIET, ils ont été jugés et le tribunal a retenu le délit de complicité dans le compte de KE et le délit d'escroquerie au moyen d'un système informatique ou d'un réseau de communication électronique en condamnant LCD, KRH et DR à cinq (5) ans d'emprisonnement chacun et à une amende de deux millions de FCFA (3 044 USD).

Source : Bénin

Typologie 5 : Fraude à la pyramide de Ponzi et blanchiment de capitaux

39. La typologie présentée ici est celle qui requiert l'attention la plus urgente compte tenu du volume et de la valeur des fonds impliqués dans les cas soumis. La typologie est liée aux actifs virtuels / crypto-monnaies ou à l'investissement en ligne. Une combinaison de cupidité et de connaissance limitée de l'entreprise proposée sont les facteurs de motivation pour la plupart des victimes vulnérables qui sont devenues la proie des schémas utilisés par ces criminels. En outre, le modus operandum utilisé ici est possible en raison de l'insuffisance du cadre réglementaire et répressif dans les États membres.

Cas 1 : Fraude à la Ponzi sur les actifs virtuels

La société «A» a été constituée à Accra en octobre 2017 avec les objets suivants qui comprennent le développement immobilier, les services de transport, le commerce électronique, les services de technologie blockchain, les transferts d'argent mobiles, la construction de routes, l'importation d'appareils à énergie solaire, les services pétroliers et gaziers. Peu après sa constitution, la société a faussement fait croire au public ghanéen qu'elle était autorisée à exercer une activité de collecte de dépôts par la Banque du Ghana, alors qu'elle n'était pas habilitée à le faire. Les escrocs ont promis à leurs victimes un rendement mensuel de 27 % sur l'investissement. La société a réussi à recevoir 43,2 millions GHS (environ 9,6 millions USD) de la part de personnes peu méfiantes. Le montant reçu a été dissipé, laissant un solde de GHS3,7 millions (USD820K) qui a été gelé par le tribunal. Au cours de l'enquête, les accusés ont admis que leur société n'était pas autorisée par la Bank of Ghana et la Securities and Exchange Commission (SEC) à exercer ce type d'activité. Ils ont également affirmé qu'ils effectuaient des transactions commerciales en ligne sur des crypto-monnaies qui se sont effondrées. L'enquête n'a pas permis d'approfondir cette affirmation, ni de la réfuter ni de la confirmer, car les enquêteurs n'avaient pas les compétences techniques requises pour vérifier la véracité des affirmations des accusés. L'enquête a toutefois établi que la société utilisait simplement le commerce des crypto-monnaies comme couverture pour obtenir des dépôts du public. En conséquence, les accusés ont été inculpés et sont poursuivis pour exploitation d'une entreprise de collecte de dépôts sans licence, escroquerie par faux semblants et évasion fiscale. Aucune charge n'a été retenue en ce qui concerne l'échange illégal de bitcoins, car l'enquête n'a pas eu l'acuité technique nécessaire pour déterminer si l'accusé était impliqué dans le commerce de crypto-monnaies et la destination des fonds. L'Office de lutte contre la criminalité économique et organisée (EOCO) a ouvert l'enquête sur la base de pétitions et de plaintes reçues de la part de certaines victimes du système frauduleux.

Source : Ghana

Cas 2 : Fraude à la Ponzi sur les actifs virtuels

En février 2020, le suspect est entré dans le pays par la route en empruntant un itinéraire non autorisé et était en possession de 10 000 USD, qu'il n'a pas déclarés comme l'exigent la loi et la réglementation. Le suspect a enregistré une entreprise individuelle à Bissau, appelée CHAVE DE SUCESSO, auprès du Centre de formalisation des entreprises du ministère de l'économie. L'Empresa Chave do Sucesso a commencé ses opérations financières en mars 2020, recevant des dépôts de particuliers avec un taux d'intérêt hebdomadaire de 20 %. Le suspect a créé un registre et formé son personnel de marketing qui mobilise les clients pour qu'ils investissent leur argent dans l'entreprise avec la possibilité de gagner 20 % de bénéfices par semaine.

Les vendeurs gagnaient 60 000 FCFA (100 USD) pour leur service et une commission supplémentaire de 3 % sur le montant déposé par chaque client qu'ils amenaient à la société. Pour convaincre ses victimes, le suspect a présenté les coordonnées de son compte bancaire domicilié dans une banque de la capitale Bissau, sur lequel il prétendait avoir effectué des transferts pour acheter de la monnaie virtuelle. Il a informé ses victimes que sa société disposait d'un compte sur la plateforme binimo.com, mais qu'en raison de la mauvaise qualité de l'Internet à Bissau, elle n'était pas active sur la plateforme.

Bien que la société suspecte soit enregistrée à Bissau, elle n'était ni enregistrée ni autorisée à recevoir des dépôts. L'enquête a révélé que le suspect a initialement payé 5,7 millions de FCFA (95 000 USD) sur les 70,8 millions de dépôts qu'il a reçus au mois de mai 2020. En juillet 2020, le suspect avait versé à 3174 investisseurs l'argent avec les intérêts respectifs d'un montant de 917 471 400 FCFA (1,53 million USD) et devait encore à 1409 investisseurs la somme de 532 249 200 FCFA (900 000 USD), y compris les intérêts cumulés de 20 % s'élevant à 443 341 000 FCFA (740 000 USD).

Le suspect a été arrêté par la police judiciaire et a saisi dans son entreprise 85 361 500 FCFA (142 000 USD). Il a été accusé de fraude, y compris de fraude fiscale et de blanchiment de capitaux. Il a été condamné à une peine d'emprisonnement de 10 ans et à rembourser à ses victimes la somme de 532.249.200 FCFA (900.000 USD). En plus du remboursement, il devra indemniser ses victimes à hauteur de 75 000 000 FCFA (125 000 USD).

Source : Guinée Bissau

Cas 3 : Fraude à la Ponzi sur les actifs virtuels

Un jeune homme ayant quelques connaissances en matière de TIC a élaboré un plan pour mettre en place un système de Ponzi. Il a effrontément diffusé des publicités et des jingles sur les médias sociaux et les radios communautaires dans les zones rurales, affirmant qu'il exploitait une entreprise de crypto-monnaie. Ses jingles et publicités promettaient 22 % d'intérêts sur le capital pendant deux semaines et 44 % tous les mois. En moins de deux mois, il a accumulé environ 5 milliards de Le (294 724,65 USD).

La CRF a fait usage de ses pouvoirs administratifs et a bloqué les fonds. La Banque de Sierra Leone a été immédiatement informée et un rapport de renseignement a été envoyé au directeur des services de lutte contre la criminalité de la police de Sierra Leone. Parmi les déposants de ce système figuraient des politiciens locaux, des officiers de police, des enseignants, des fermiers, des étudiants, etc.

Les investigations ont révélé qu'il possédait un portefeuille de crypto-monnaies qui ne contenait que 800 dollars. Les investigations ont également révélé qu'il n'était pas engagé dans le commerce des crypto-monnaies mais dans un système de Ponzi. La Haute Cour est saisie de cette affaire.

Source : Sierra Leone

Cas 4 : Fraude à la Ponzi en ligne

VH est un jeune homme d'affaires qui a l'habitude d'effectuer des retraits fréquents en utilisant le service d'argent mobile. Il effectue quotidiennement des retraits importants à partir de différents points de retrait d'argent mobile. Pour effectuer ses transactions, il possède plusieurs cartes SIM. Lorsque l'une des cartes sim a atteint la limite de retrait autorisée, il la remplace par une nouvelle pour poursuivre les opérations. Ces activités fréquentes ont éveillé les soupçons de l'opérateur, qui a d'abord pensé à un dysfonctionnement de sa plateforme. Afin de confirmer ses soupçons, l'opérateur a déposé une plainte auprès du chef de file de la lutte contre la cybercriminalité (PLCC). Le PLCC, appuyé par le Digital Forensics Laboratory, a entamé des investigations qui ont abouti à l'arrestation de VH. Amené dans les locaux et interrogé, il a déclaré appartenir à un réseau et avoir été recruté pour effectuer des retraits avec des cartes sim mises à sa disposition. Les fonds retirés, a-t-il dit, provenaient d'un site d'investissement boursier en ligne appelé ANTP dont le lien est : https://www.antp.io. Ce site invite les particuliers à investir un montant de leur choix pour obtenir un meilleur retour sur investissement. L'argent investi devait fructifier en fonction du nombre de tâches quotidiennes à effectuer sur le site. Les membres ne se doutaient pas de la supercherie. En effet, ils ont constaté l'augmentation de leur solde sur la plateforme comme promis. Cependant, quelques jours plus tard, ils ont été bloqués et n'ont pratiquement pas reçu leur dû. A l'exception de quelques-uns qui ont reçu de l'argent sur leur compte de trading mobile afin de les pousser à investir davantage et d'attirer le plus grand nombre de personnes. Suite à la perquisition et à la saisie, la PLCC a arrêté 12 membres du réseau. Il s'agit de ZQ, XC, KY, MK, TBF, SL, SAM, MT, ME, MA, KKY, MM. Ils avaient en leur possession des centaines de téléphones, 08 ordinateurs portables et la somme de 46 553 000 francs CFA (75 000 USD).

Le préjudice provisoire a été estimé à plus de 1 000 000 000 de francs CFA (1,6 million USD). Plusieurs transactions ont été effectuées et les fonds déposés sur un compte bitcoin pour contourner les mécanismes. (l'affaire était en cours au moment de la présente étude)

Source : Côte d'Ivoire

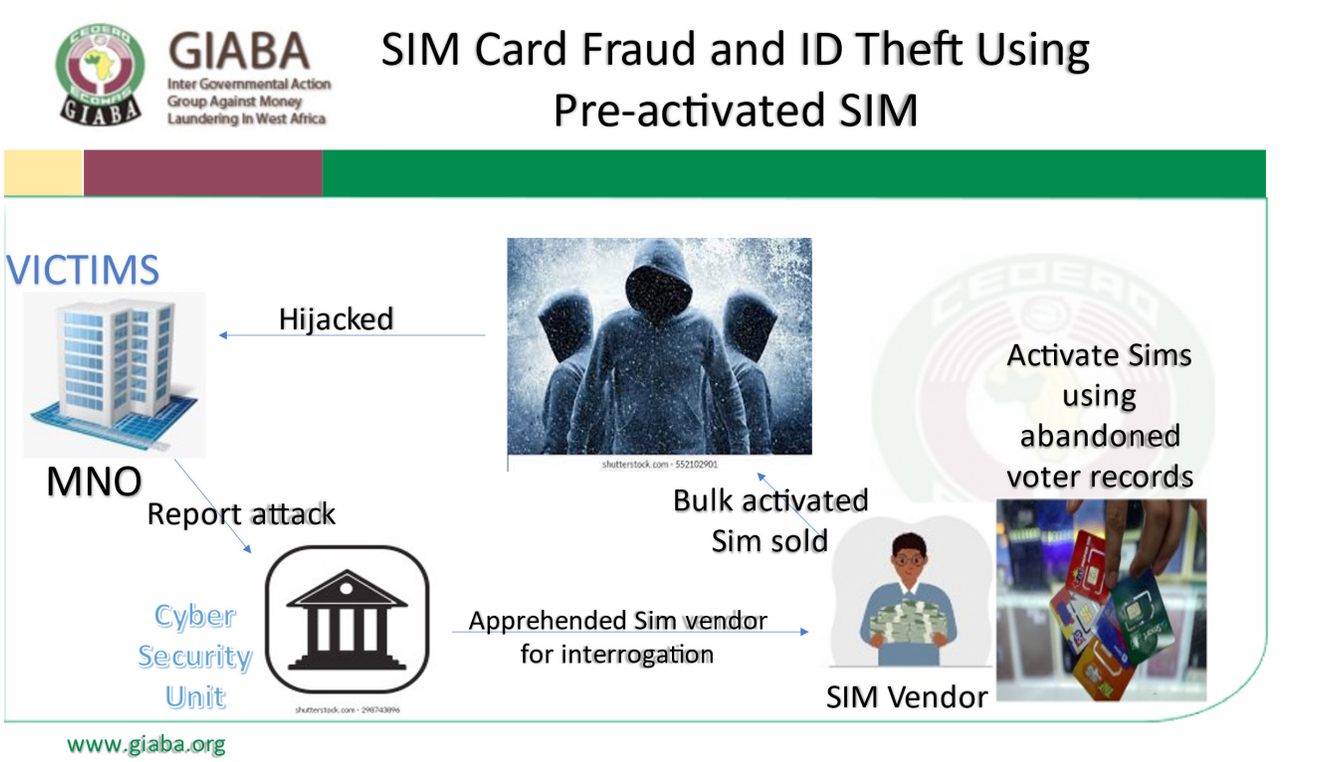
Méthodes et techniques

- Création d'un site Internet de type «Ponzi» avec des fonctionnalités de plateforme d'échange et d'investissement en ligne.
- Permettre au site web de s'afficher sur la page des médias sociaux des victimes potentielles.
- Verser une partie du paiement aux victimes/investisseurs initiaux pour les inciter à investir davantage et pour que d'autres personnes fassent confiance au processus.
- Les faux augmentent le retour sur investissement des victimes/investisseurs pour les inciter à investir davantage.

Drapeaux rouges et indicateurs

- Opportunités d'investissement non F2F avec des start-ups en ligne.
- Offre commerciale irréaliste - Super profit grâce à un retour sur investissement très élevé.

Titre : version française *(à envoyer)*



Cas 5 : Fraude à la pyramide de Ponzi par investissement dans l'argent mobile

En 2022, un cas de faux investissement a été signalé à la brigade des fraudes de la police gambienne par 146 victimes. Un soi-disant investissement appelé Qubid a été introduit en Gambie par un nom fictif, Marcus Gabel, qui se trouverait au Nigeria. Il a recruté des agents en Gambie pour mener à bien la prétendue forme d'entreprise. La nature de l'entreprise est que l'agent encourage les gens à investir avec eux par le biais de l'argent mobile et des dépôts bancaires et à recevoir leur capital et 20 % d'intérêt après sept jours.

Le premier groupe de personnes ayant investi a reçu ses différents intérêts, ce qui a encouragé de nombreuses personnes à investir dans l'entreprise. Un montant total de 24 526 993 D (437 982 USD) a été investi dans l'entreprise par 146 personnes. Une partie de l'argent investi a été utilisée pour payer le capital et les intérêts des investisseurs dont l'investissement était arrivé à échéance. L'un des agents a envoyé un montant de D2 834 000 (50 607 USD) en bitcoins et D551 125 (9 841) à Marcus au Nigeria. Cet argent était censé constituer les fonds d'investissement.

L'enquête a révélé que ladite société n'avait jamais été enregistrée en Gambie et que celui qui avait lancé l'affaire se trouvait au Nigeria et qu'il gérait/contrôlait l'affaire par l'intermédiaire d'un groupe WhatsApp. Les quatre agents ont été inculpés de blanchiment de capitaux, d'obtention d'argent sous un faux prétexte et d'exercice d'activités bancaires en Gambie sans licence. Ils sont actuellement jugés par la Haute Cour de Gambie.

Source : Gambie

Cas 6 : Fraude à l'investissement dans le commerce électronique

Au cours de l'année 2019, la Brigade centrale de lutte contre la cybercriminalité (BCLCC) a reçu plusieurs victimes qui souhaitaient porter plainte contre la société Chymall pour escroquerie et abus de confiance ayant causé un préjudice de plus d'un milliard de francs CFA.

De l'audition du chef d'entreprise, il ressort que la société a adhéré à une plateforme de commerce en ligne dénommée SAIRUI. Avec l'évolution de leur activité, ils ont été promus centre moyennant le paiement d'une somme de dix mille (10.000) dollars. Leur position de centre a fait d'eux des intermédiaires par lesquels d'autres personnes pouvaient adhérer à cette plateforme, recevoir les produits et leurs éventuels bonus. En juin 2020, suite au changement de dénomination de la société devenue Chymall, une représentation a été créée au Burkina Faso. Ils ont alors commencé à inscrire d'autres personnes qui souhaitent rejoindre la plateforme, sous le parrainage des dirigeants. Les choses se sont déroulées normalement pendant un certain temps et les personnes qui accédaient à la plateforme par l'intermédiaire de leur centre ont commencé à recevoir leurs primes conformément aux tarifs fixés par Chymall. Cependant, en novembre 2020, ils ont commencé à faire face à des problèmes de paiement et à des anomalies qui ne respectaient pas les règles préétablies. Aussi, tous les comptes de la plateforme ont subi un changement.

Une enquête plus approfondie a révélé que la société mère était basée en Chine et avait une représentation au Ghana. À ce jour, nous comptons plus de mille (1000) victimes dont les dommages s'élèvent à plus d'un milliard de francs CFA (1,6 million USD).

Source : Burkina Faso

Cas 7 : Fraude au prêt en ligne / sans contact direct avec le client

M. AS s'adonne à la cybercriminalité en postant des messages de prêt en ligne sous de fausses identités afin d'escroquer ses victimes. L'enquête a conduit à l'arrestation d'AS, résidant à Abomey-calavi, dans l'arrondissement de Bidossessi, en septembre 2019. Suite à son arrestation, AS a été retrouvé avec de faux documents relatifs à des contrats de prêt, des ordres de virement, des attestations de garantie d'assurance, des copies de transfert d'argent retrouvés dans son téléphone et son ordinateur portable en sa possession. Il a déclaré avoir utilisé les fonds extorqués aux victimes pour acheter un véhicule, ouvrir un magasin de vêtements et faire d'autres investissements. Il a ordonné à ses victimes de verser des avances sur les frais de garantie des prêts sur les comptes bancaires appartenant à ses complices qui, à leur tour, effectuent des retraits. Le procureur spécial de la CRIET a été saisi de l'affaire en septembre 2022. AS a été jugé et condamné à cinq (5) ans d'emprisonnement et à une amende de cinq cents (761 USD). Tous les biens liés à l'affaire ont été confisqués.

Source : Bénin

Typologie 6 : Fraude et blanchiment de capitaux liés à l'argent mobile

40. La fraude liée à l'argent mobile est la deuxième typologie la plus répandue en Afrique de l'Ouest, après la fraude aux avances de frais. La ligne de démarcation entre la fraude aux avances de frais et les autres fraudes liées à l'argent mobile est mince. En fait, presque toutes les fraudes aux avances de frais sont rendues possibles par le téléphone mobile et, dans la plupart des petits et moyens paiements, la plateforme d'argent mobile est utilisée pour recevoir les avances de frais demandées ou exigées. Certains des cas présentés comme des fraudes aux avances de frais peuvent également être présentés comme des fraudes liées à l'argent mobile.

Cas 1 : Faux-semblants, usurpation d'identité, falsification et fraude à l'argent mobile

Une succursale du service clientèle d'une banque a reçu un appel censé provenir du siège social de la banque. L'appelant s'est présenté comme un membre du comité exécutif (EXCO Member) en utilisant le nom de Chief Operating Officer (COO). Après une brève conversation téléphonique avec le responsable du service clientèle, il a demandé à parler au caissier qui s'occupe des opérations de Mobile Money dans l'agence. L'appel a été transféré au guichetier, à qui il a indiqué qu'il souhaitait lui expliquer comment effectuer des inversions de paiement par téléphone portable sur la plateforme Momo. Il a ensuite demandé à la caissière d'entrer son code PIN MoMo et, après avoir entré le code PIN, le suspect a donné une série d'instructions que la caissière a suivies. Immédiatement après que le suspect ait raccroché, la guichetière a remarqué qu'un montant total de 37 000 GHS (6 491 USD) avait été transféré frauduleusement du portefeuille de la banque à celui d'un particulier, qui l'a immédiatement retiré.

L'affaire a été signalée à la police qui, avec l'aide de MTN Ghana, a retrouvé le suspect, un homme de 30 ans, dans sa cachette située dans une ville éloignée et a été arrêté en mars 2021. Au cours de l'enquête, il a été établi que la carte d'identité utilisée par le suspect pour enregistrer sa carte SIM était fausse. Le suspect a été inculpé pour contrefaçon, usurpation d'identité, escroquerie sous de faux prétextes et blanchiment de capitaux. Les poursuites sont toujours en cours au tribunal de circuit.

Source : Ghana

Cas 2 : Faux-semblants, usurpation d'identité, falsification et fraude à l'argent mobile

Un suspect, M. ABD, a été arrêté en juillet 2021, soupçonné d'escroquerie par le biais des médias sociaux. Le suspect et d'autres complices utilisaient Facebook et Messenger sous un faux nom de profil (SOIOIO MELA) et trompaient astucieusement leurs victimes en leur extorquant de l'argent. En plus de Facebook Messenger, il utilisait également des numéros de téléphone portable enregistrés au nom d'autres personnes pour communiquer avec ses victimes. Les enquêtes préliminaires ont conduit la police à deux personnes qui ont eu un contact visuel avec le suspect, car il leur avait demandé d'utiliser leurs numéros de téléphone portable pour recevoir de l'argent qui lui était transféré. Ces personnes ont confirmé qu'elles le reconnaîtraient si elles le rencontraient. L'enquête a rapproché les informations susmentionnées des déclarations faites par M. BILL, communément appelé SOIOIO, lorsqu'il a accompagné l'une des victimes pour déposer la plainte auprès de la police. M. BILL a confirmé à l'enquête que le suspect est un individu communément appelé SACA, qui, en collusion avec sa nièce nommée SC, avait utilisé son téléphone portable, que sa nièce avait volé à sa résidence à Bula, avec lequel ils avaient commis des actes similaires et mis sa réputation en question, car ils demandaient de l'argent en son nom, et envoyaient des messages d'amour à ses amis et connaissances, jetant le discrédit sur les relations matrimoniales de certaines des personnes qu'ils avaient ciblées. Il a toutefois pu récupérer son téléphone portable grâce à l'intervention de la police judiciaire.

Le suspect était sous la garde du ministère public, prêt à être jugé par la section criminelle du tribunal régional de Bissau, en attendant l'expertise du téléphone portable (Infinix Smart Dual Camera) qui lui a été confisqué.

Source : Guinée Bissau

Cas 3 : Faux-semblants, usurpation d'identité et fraude à l'encontre d'un agent de transfert de fonds par téléphone mobile

En février 2018, un tribunal de district à Oda, dans la région orientale du Ghana, a emprisonné deux personnes âgées respectivement de 28 et 29 ans pour avoir escroqué un agent de mobile money. Selon la police, les suspects ont appelé l'agent de l'argent mobile sur le téléphone et ont prétendu qu'ils étaient des agents de MTN Ghana Ltd appelant pour éduquer l'agent sur sa transaction d'argent mobile. Cependant, au cours de la transaction, l'agent a remarqué que son compte avait été débité de 2000 GHS. L'agent a signalé l'incident à la police, qui a assuré la liaison avec MTN et a fait en sorte que les suspects soient retrouvés et arrêtés. L'un des suspects prétendait être un expert en technologies de l'information et de la communication (TIC) et l'autre était sans emploi. Les deux suspects ont été poursuivis et emprisonnés.

Source : Ghana

Cas 4 : Opérations d'initiés, piratage utilisant un système d'ingénierie complexe et fraude à l'argent mobile

Bank X au Ghana a déposé une requête auprès de l'EOCO pour des retraits non autorisés effectués sur les comptes d'un certain nombre de ses clients via les plateformes de banque mobile et de banque en ligne de la banque. Les retraits frauduleux ont été effectués alors que les clients étaient en train de se familiariser avec les services bancaires électroniques. Avant la requête de la banque X, deux autres banques, Y et Z, avaient également déposé des plaintes similaires concernant des retraits non autorisés effectués par certains de leurs clients via l'application de banque mobile et quatre suspects ont été arrêtés par l'EOCO. L'enquête a révélé que les attaquants mettaient en œuvre des programmes complexes d'ingénierie sociale destinés à des personnes peu méfiantes afin d'obtenir les identifiants de connexion aux portails bancaires électroniques. Certains des suspects avaient obtenu des détails sur les clients (notamment le numéro de compte, le nom du compte, le solde du compte, la date de naissance, l'adresse et les numéros de téléphone) de la part de co-conspirateurs de certaines banques. Munis de ces informations, ils ont appelé les clients avec des numéros clonés qui semblaient provenir des banques et ont incité les victimes à donner leurs coordonnées. Une fois ces informations d'identification obtenues, les fonds ont été superposés et blanchis grâce à un système élaboré comprenant l'utilisation de plusieurs comptes d'argent mobile et de comptes bancaires d'agents tiers. Dans certains cas, quelques instants après les retraits non autorisés, les fonds étaient immédiatement retirés de Mobile Money Merchants. L'enquête est toujours en cours.

Source : Ghana

Cas 5 : Délits d'initiés, usurpation d'identité et fraude à l'argent mobile

En avril 2022, l'EOCO a arrêté un responsable de banque et un employé d'un grand réseau de télécommunications qui auraient été de connivence avec quatre personnes pour escroquer des clients de banque par le biais d'une fraude à l'échange de cartes SIM. Les suspects ont demandé à l'employé de banque de leur fournir les détails des comptes bancaires et les numéros de téléphone de leurs victimes ayant d'importants soldes de comptes afin de les aider à retirer des fonds de leurs comptes, tandis que le personnel de la société de télécommunications a été contacté pour cloner les numéros de téléphone des victimes dans le cadre de l'opération. Le personnel de la banque s'est entendu avec les accusés en leur fournissant les détails demandés et ils ont pu cloner les numéros de téléphone de trois clients dans l'intention de leur voler respectivement 850 000, 680 000 et 50 000 GH¢ (soit un total de 216 000 USD). Les accusés ont créé une application mobile avec les cartes SIM clonées pour retirer les fonds des comptes bancaires des clients. Entre-temps, le fonctionnaire de la banque a informé la banque de la machination et le problème a été signalé à l'EOCO. Les accusés ont été arrêtés alors qu'ils tentaient de retirer les fonds de la banque. Ils ont été inculpés de neuf chefs d'accusation pour conspiration de vol, tentative de vol et participation à un groupe criminel organisé. L'affaire fait l'objet de poursuites judiciaires.

Source : Ghana

Cas 6 : Usurpation d'identité, fraude à l'argent mobile et à la carte SIM

M. O, jeune diplômé, a créé sa propre entreprise de vente de cartes SIM afin d'acquérir une indépendance financière. Son affaire marchait bien jusqu'au jour où il a été approché par KDU qui lui a demandé d'acheter 5 cartes Sim. L'idée est de les utiliser pour ouvrir cinq agences de transfert mobile. M. O a activé les cartes SIM et, comme d'habitude, le client a été satisfait. Alors qu'il poursuit son activité, M. O apprend que les cartes Sim qu'il a vendues à KDU ont été utilisées dans des transactions frauduleuses. Il est surpris car KDU lui avait dit que les cartes étaient destinées aux cinq caissiers des agences qu'il était sur le point d'ouvrir. KDU avait fourni à M. O cinq identifiants différents pour l'activation des cartes SIM. Il était inquiet car il avait également entendu des rumeurs selon lesquelles l'escroquerie du portefeuille électronique était en cours. De plus, il a été convoqué quelques semaines plus tard par la police spécialisée dans la cybercriminalité pour une affaire similaire. En effet, la Plateforme de lutte contre la cybercriminalité (PLCC) est actuellement submergée de plaintes liées à ce délit. Parmi elles, celles de trois victimes LLF, CNS et MYL qui affirment avoir été contactées par téléphone par des inconnus. Elles affirment avoir effectué des dépôts par erreur sur leurs numéros. Pour vérifier l'effectivité des transactions alléguées, les victimes ont vidé leur portefeuille au profit d'un numéro inconnu. Chacune d'entre elles a déposé une plainte auprès de la PLCC afin de résoudre l'affaire.

L'enquête du PLCC, soutenue techniquement par le LCN (Digital Forensics Laboratory), a permis de découvrir que le numéro recevant les transferts appartenait à KDU. Le suspect a été arrêté et était en possession de 27 cartes Sim. Lors de son interrogatoire, KDU a reconnu avoir escroqué plusieurs personnes sur leurs comptes mobiles avec les puces achetées à M. O. L'analyse des 27 cartes Sim par le LCN a également révélé qu'elles avaient été utilisées pour d'autres transactions frauduleuses. Ces numéros ont fait l'objet de 136 plaintes et ont effectué 308 dépôts frauduleux pour un montant de 12 786 202 francs CFA (19 520 euros).

Finalement, KDU a été déféré devant le parquet d'Abidjan où il pourrait être poursuivi pour escroquerie et complicité d'escroquerie à la transaction. (L'affaire était en cours au moment où elle était rapportée)

Source : Côte d'Ivoire

Cas 7 : Délits d'initiés et fraude aux agents de l'argent mobile

En janvier 2022, la Brigade centrale de lutte contre la cybercriminalité a été contactée par le gérant de la société C2EGF-BF qui a déposé une plainte contre l'un de ses commerciaux pour faux et usage de faux, abus de confiance et blanchiment de capitaux ayant causé un préjudice de plus de trente-sept millions de francs CFA (60 000 USD).

Il ressort de l'enquête que le défendeur a été recruté par la société C2EGF-BF en tant que représentant commercial. La société est un distributeur de Mobile Money. Le travail de l'accusé consistait à recruter, former et assister les agents des points de vente de la société. Ce dernier a profité de sa position commerciale pour installer une dame et celle-ci a appelé au niveau de la société pour demander des fournitures. Les reçus justifiant les remboursements passaient par ce dernier.

Une enquête plus approfondie a conduit à l'arrestation du suspect. Il prenait un ancien ticket de caisse, changeait la date, prenait une photo et l'envoyait à l'entreprise via WhatsApp en tant que message instantané. Dès que le message est lu, il est immédiatement supprimé. Le mis en cause a utilisé l'argent de son forfait pour créer plusieurs autres boutiques orange money au nom de ses parents et de ses copines. (L'affaire était en cours au moment où elle était rapportée)

Source : Burkina Faso

Cas 8 : Fraude à la carte Sim et usurpation d'identité à l'aide d'une carte Sim préactivée provenant de dossiers d'électeurs abandonnés

Le réseau informatique d'une entreprise a été piraté. Le pirate a exploité les failles de sécurité du réseau et des applications de l'entreprise pour extraire de l'argent du système de monnaie électronique. En effet, une puce de test pour de nouveaux services a été mise en place dans un département sans mesures de suivi en cas d'incident pour déterminer les responsabilités.

La puce a été utilisée pour positionner de l'argent sur plus de 100 comptes en monnaie électronique. La traçabilité de l'argent est rendue difficile par le fait que l'identification et la vente des puces ne sont pas très bien encadrées. Ainsi, l'argent de cette attaque est retiré dans différents magasins de plusieurs villes, notamment Dakar et Thiès. Le détail des opérations suggère l'utilisation d'un moyen de transport pour retirer l'argent dans tous les magasins de l'axe Dakar-Thiès.

Une enquête a été ouverte à la suite d'une plainte déposée par l'entreprise attaquée. Il a été constaté que différentes puces avaient été activées au préalable sans qu'il soit possible d'établir l'identité des véritables propriétaires. Ces mêmes puces ont ensuite été utilisées pour ouvrir des comptes en monnaie électronique.

Les enquêtes menées au sein de la structure n'ont pas permis de déterminer l'origine de la connexion qui a réalisé ces opérations frauduleuses. De plus, aucun système de validation des opérations ou de veille sur les opérations importantes n'a été mis en place. L'enquête s'est donc orientée sur la piste des jetons afin d'établir l'identité des véritables propriétaires afin d'identifier le destinataire final de ses opérations. Ainsi, le vendeur qui a procédé à l'activation des différentes puces a été interrogé. N'étant pas en mesure de fournir l'identité des acheteurs, une perquisition a été effectuée à son domicile. Il a ainsi été découvert qu'il avait lui-même procédé à l'activation des différentes puces sur base des données personnelles contenues dans le fichier électoral. En effet, après chaque élection, les fichiers sont récupérés et vendus sur le marché. Ceci constitue une faille majeure dans l'application de la mesure imposant aux opérateurs téléphoniques d'identifier leurs clients.

Source : Sénégal

Méthodes et techniques

- Utilisation de fausses identités pour usurper l'identité de personnes ou d'entités
- Les escrocs se font passer pour des agents du service clientèle et demandent aux utilisateurs de partager leurs codes PIN, OTP (mots de passe à usage unique) ou les détails de leur compte en prétendant aider le client à « résoudre un problème ».
- Utilisation de numéros de téléphone mobile enregistrés au nom d'autres personnes
- Utilisation de schémas complexes d'ingénierie sociale pour obtenir des identifiants de connexion à la plateforme électronique de personnes physiques ou morales.

Drapeaux rouges et indicateurs

- Un compte d'argent mobile reçoit ou envoie soudainement d'importantes sommes d'argent, en contradiction avec l'activité précédente.
- Plusieurs transactions de grande valeur dans un court laps de temps.
- Les fonds sont immédiatement retirés ou transférés sur plusieurs comptes dans les minutes qui suivent leur réception.

Série de transferts de fonds d'un portefeuille ou d'un compte vers plusieurs comptes ou portefeuilles à intervalles rapprochés.

Typologie 7 : Cas de financement du terrorisme par la cybernétique

41. Comme le financement du terrorisme reste un phénomène complexe auquel la région est toujours confrontée, en particulier pour comprendre le modus operandi dont on pense qu'il se produit en grande partie dans le secteur informel et peut-être en utilisant le cyberespace, y compris le dark web, il y a trois cas soumis qui se qualifient comme des cas de financement du terrorisme activés par la cybernétique.

Cas 1 : Financement du terrorisme par le commerce

Un citoyen canadien d'origine somalienne résidant à Dakar avait créé une société immobilière au Sénégal. Cette société, en collaboration avec un Sénégalais, avait ouvert un compte auprès d'une banque à Dakar. Quelque temps plus tard, le compte a reçu un transfert d'environ cent six mille (106 000) dollars américains d'un ressortissant somalien résidant aux États-Unis. Le transfert a été exécuté par une institution financière basée à Dubaï. Soupçonnant cette opération, en raison de l'identité peu documentée du nouveau client et de la destination des fonds, la banque sénégalaise a effectué une déclaration de soupçon auprès de la CRF. L'enquête a révélé que la société n'avait aucun statut légal au Sénégal et qu'elle avait été créée spécifiquement dans le but de blanchir des fonds illicites par la vente de marchandises importées. En outre, les personnes impliquées étaient en contact avec des groupes extrémistes impliqués dans des activités terroristes en Afrique de l'Est, en Amérique et en Afrique de l'Ouest. D'autres sociétés ont été créées, en association avec des Sénégalais, pour importer des biens d'occasion, dont une partie était vendue à Dakar et l'autre exportée vers un autre pays pour y être revendue. Le produit de ces différentes opérations commerciales a ensuite été envoyé à plusieurs groupes terroristes par divers canaux. (l'affaire était en cours au moment de la présente étude)

Source : Sénégal

Cas 2 : Suspicion de collecte de fonds pour le financement du terrorisme

En 2015, la banque XPTO a déposé une DOD concernant une personne identifiée par XMAN, de nationalité turque, résidant à Praia et enseignant indépendant. Ses transactions financières comprennent des retraits et des transferts de devises à l'étranger, et il reçoit également des fonds provenant spécifiquement de Turquie. Il a été constaté que les paiements étaient compensés par le titulaire du visa pour des montants égaux aux crédits déposés en espèces le jour même ou le lendemain. Opération d'achat de devises étrangères pour un montant considérablement élevé sans justification, étant donné que le client est un enseignant indépendant comme il l'a déclaré à la banque XPTO.

Mouvement de compte caractérisé par de nombreux petits montants créditeurs et un petit nombre de débits de grande valeur. La justification donnée par XMAN quant à l'utilisation des fonds à des fins religieuses ne correspond pas aux paiements effectivement effectués pour des services de communication, des logements et des voyages fréquents. Absence de relation raisonnable entre XMAN et la société PPP, dont l'objet est la vente de matériel informatique.

Après analyse de la DOD de la banque XPTO, il a été constaté que M. XMAN est titulaire de deux comptes distincts (en devises nationales et étrangères), auprès de la banque en question, ouverts respectivement en septembre et en décembre 2012. Pour le compte ouvert en décembre 2012, il a reçu des transferts de la banque turque KATILIM BAKAST A. S., d'un montant total de 5 669 379$00 Escudos CV (51 416 euros), en (04) quatre mouvements, les motifs des transferts étant le paiement du Qurban (sacrifice d'animaux) et à des organisations d'orphelinat. Les montants reçus par le biais des transferts indiqués ci-dessus, entre janvier et mai 2014, ont été utilisés par M. XMAN pour effectuer des paiements avec des chèques bancaires XPTO pour la subsistance et les voyages, et non à des fins religieuses et caritatives comme indiqué dans les transferts. Les paiements ont été effectués à la société PPP qui vend du matériel et à la société QQQ qui importe divers produits alimentaires, ainsi qu'à une agence de voyage.

Entre 2013 et 2014, M. XMAN a effectué plusieurs voyages, dont 9 (neuf) entre PRAIA/DAKAR, 4 (quatre) entre PRAIA/MOROCCO, 5 (cinq) entre PRAIA/PORTUGAL et 1 (un) PRAIA/BISSAU. Le cas en question fait toujours l'objet d'une enquête.

Source : Cabo Verde

Cas 3 : Financement du terrorisme par des transferts informels (HAWALA)

En 2022, les services de sécurité de l'Etat ont mis à la disposition des services d'enquête M. DA, transporteur et trafiquant de motos, soupçonné d'être un collaborateur d'un groupe armé terroriste dirigé par M. IL. IL est un criminel recherché, cité dans plusieurs affaires d'extorsion, de pillage et de violences graves contre des civils au Niger, y compris son implication dans des activités terroristes dans le Liptako Gourma. IL, selon les sources d'information, dirige un groupe armé qui commet des actes qualifiés de terroristes par la législation nigérienne.

D'après l'enquête, IL utilisait un faux nom, une fausse pièce d'identité et un numéro de téléphone non identifié pour envoyer fréquemment de l'argent depuis son domicile vers une destination à DOUT, une ville frontalière située dans le sud du pays, une zone relativement sûre où se trouvent de nombreux trafiquants de toutes sortes. Il transfère les fonds à DA en utilisant Hawala. Une fois le transfert effectué, DA reçoit un message d'alerte sur son téléphone indiquant le dépôt de fonds effectué en son nom. Il reçoit également un appel téléphonique du Sieur IL confirmant le montant de l'argent envoyé. DA a retiré les fonds, puis s'est rendu dans la ville frontalière proche du DOUT pour acheter des motos et les livrer dans la zone où IL opère.

En plus des fonds (500 000 FCFA / moto) destinés à l'achat des motos, DA reçoit un supplément de 50 000 à 60 000 FCFA (100 USD) par moto convoyée jusqu'à la frontière nord-ouest du Niger.

Source : Niger

CHAPITRE 4

SIGNAUX D'ALARME ET INDICATEURS

42. Ce chapitre, qui découle du précédent, présente les signaux d'alerte et les indicateurs observés dans les cas présentés. Les signaux d'alerte et les indicateurs sont des activités ou des actions qui sous-tendent certaines activités, actions, transactions ou événements, avec certaines anomalies qui suscitent la suspicion et/ou des incohérences lorsqu'elles sont soumises à un examen rationnel. Ces anomalies ou incohérences conduisent à des soupçons qui nécessitent un examen plus approfondi, une interrogation, une enquête ou, à tout le moins, une surveillance par les entités déclarantes, les superviseurs et le public. L'analyse des cas présentés dans le chapitre précédent a permis d'identifier un certain nombre d'indicateurs et de signaux d'alerte possibles. Ces indicateurs et signaux d'alerte diffèrent selon l'ampleur des activités de blanchiment de capitaux ou de financement du terrorisme. Alors que les indicateurs représentent des événements qui peuvent ou non indiquer l'existence d'un blanchiment de capitaux ou d'un financement du terrorisme, les signaux d'alerte représentent des événements qui fournissent des preuves solides ou plus claires d'un blanchiment de capitaux ou d'un financement du terrorisme.

43. Vous trouverez ci-dessous une liste non exhaustive d'indicateurs et de signaux d'alerte identifiés à partir de l'analyse de l'ensemble des cas. Les indicateurs et les signaux d'alerte confirment que les informalités, le manque de sensibilisation du public aux cybermenaces, l'insuffisance des ressources investies dans la cybersécurité par les entreprises et les institutions/organisations publiques, la faiblesse de l'architecture, des systèmes réglementaires et de la surveillance du paysage cybernétique dans la région, ainsi que la faiblesse des systèmes d'application de la loi ont un effet d'entraînement sur la cybercriminalité et la cybercriminalité assistée, le blanchiment de capitaux et le financement du terrorisme en Afrique de l'Ouest.

Indicateurs

- Une entreprise cliente ayant une relation établie modifie les coordonnées du compte du bénéficiaire (par exemple, le code IBAN) pour un bénéficiaire connu.

- Il y a une incohérence entre le nom du bénéficiaire dans les instructions de paiement et dans les détails du compte (par exemple, le code IBAN).

- Utilisation de services informels de transfert de fonds (tels que les services de type «Hawala») pour les transferts transfrontaliers.

- Inadéquation entre l'activité économique et le fonds en question, qu'il s'agisse de transferts de fonds ou de transactions bancaires.

- Différences dans l'orthographe du nom du bénéficiaire par rapport à ce qui figure sur les documents d'identification produits pour les retraits.

- Utilisation de services de transfert de fonds ou de valeurs ou de prestataires de services de remise de fonds pour recevoir des fonds de clients non liés.

- Utilisation de mules (hommes de paille), de comptes de paille, de courriers, etc. pour transférer des fonds.

- Le compte du bénéficiaire peut appartenir à une société offshore ou être détenu par une institution financière située dans une juridiction à haut risque, selon la décision de l'institution financière et des autorités compétentes concernées.

- Paquet prétendument envoyé par un ami en ligne qui demande de payer un certain montant avant de le recevoir.

- On vous demande d'investir par le biais de l'argent mobile dans une société suspecte qui n'est pas enregistrée ou qui n'a pas de bureau dans le pays.

- Le client demande qu'une transaction (paiement) soit effectuée d'urgence ou qu'elle soit traitée de manière confidentielle.

- Les instructions de paiement sont reçues d'un nouvel employé de l'entreprise cliente.

- Transactions inhabituelles et de grande valeur commandées uniquement par e-mail.

- Demandes de modification d'un compte bancaire de bénéficiaire effectuées peu de temps après une commande initiale (surtout si elles sont effectuées par e-mail).

- L'entreprise cliente ayant une relation d'affaires établie demande qu›un paiement soit effectué à un bénéficiaire suspect pour la première fois.

- La transaction est liée à l'achat ou à la vente de monnaie virtuelle (par exemple, Bitcoins, Litecoin, Ethereum, Zcash) ou d'actifs virtuels similaires.

- Le client demande qu'une transaction soit effectuée en urgence ou qu'elle soit traitée de manière confidentielle, surtout si elle est juste avant les heures de fermeture, les week-ends ou les jours fériés.

- Retraits d'espèces ou transactions déboursant un montant reçu, effectués peu de temps après un dépôt d'un montant reçu de l'étranger, ou sous un titre peu clair et inhabituel.

- Le client qui commande le versement d'un paiement à un bénéficiaire ne communique avec le bénéficiaire que par courrier électronique.

- Transaction qui entraîne une activité importante, mais inexplicable, sur le compte qui était auparavant principalement inactif ou dont le taux de rotation du compte était faible.

Drapeaux rouges

- Envois réguliers de fonds par plusieurs expéditeurs au même destinataire ou à des personnes liées, y compris les envois de fonds par un ou plusieurs expéditeurs dans différents pays à un destinataire local. En particulier, lorsque le destinataire n'a aucune relation avec les expéditeurs.

- Envois de fonds sur une courte période et structurés juste en dessous du seuil de déclaration qui, ensemble, représentent une somme d'argent importante.

- Entrée soudaine de fonds en espèces suivie d'une sortie soudaine par le biais d'instruments financiers tels que les chèques.

- Une institution financière reçoit un virement pour créditer un compte, mais le virement désigne un bénéficiaire qui n'est pas le titulaire du compte. Cela peut correspondre à des cas où une victime envoie involontairement des virements électroniques vers un nouveau numéro de compte fourni par un criminel se faisant passer pour un bénéficiaire, un fournisseur ou un vendeur connu.

- Utilisation de services de remise pour le paiement de biens et de services commandés en ligne.

- Message envoyé sous le couvert d'une promotion d'un opérateur téléphonique et le destinataire est invité à saisir son code PIN comme mesure de vérification pour réclamer son «prix».

- Réception d'un SMS indiquant un dépôt sur le compte d'un client, puis réception d'appels indiquant que le dépôt était une erreur et qu'il fallait renvoyer le montant.

- Réception d'un appel d'une société de livraison sous le prétexte de livrer des marchandises d'amis/de parents à l'étranger. On vous demande alors de verser de l'argent sur un compte mobile money pour le service de livraison.

- Proposition commerciale attrayante et trop belle pour être vraie, émanant d'une prétendue connaissance qui souhaite que vous remplaciez un fournisseur de produits locaux très demandés à l'étranger.

- Demande de participation ou d'investissement dans des entreprises qui offrent des rendements super normaux

- Réception d'un courriel contenant un lien suggérant que votre compte a été piraté, que vos photos de nu sont sur Internet, que votre proche a besoin de soins médicaux immédiats ou qu'un autre type de chantage ou de cyber-attaque est sur le point de se produire et que vous devez suivre certaines instructions, y compris cliquer sur le lien qui vous a été envoyé.

- Une demande inhabituelle de la part d'un ami ou d'un parent vous demandant une aide financière d'urgence et vous invitant à ne communiquer que par messages.

- Les messages relatifs à l'admission, au recrutement ou au gain d'un prix dans le cadre d'un jeu en ligne auquel vous n'avez pas participé peuvent constituer une attaque par hameçonnage ou même le recrutement d'un groupe terroriste.

- Requêtes reçues demandant à une personne de mettre à jour ses données personnelles associées à des informations bancaires et autres.

- Un compte d'argent mobile reçoit ou envoie soudainement d'importantes sommes d'argent, ce qui n'est pas conforme à l'activité précédente.

- Les fonds sont immédiatement retirés ou transférés sur plusieurs comptes dans les minutes qui suivent leur réception.

- Série de transferts de fonds d'un portefeuille ou d'un compte vers plusieurs comptes ou portefeuilles à intervalles rapprochés.

CHAPITRE 5

CADRE JURIDIQUE, RÉGLEMENTAIRE, DE SURVEILLANCE ET D'APPLICATION ET DÉFIS ASSOCIÉS

44. Ces dernières années, l'Afrique de l'Ouest a connu un essor considérable de son cyberespace et de l'utilisation de cet espace, ce qui a entraîné une croissance des entreprises, de la rentabilité et de l'efficacité dans la mise en œuvre et l'exécution des programmes. La région a également souffert d'une augmentation exponentielle de la cybercriminalité, en particulier de la cybercriminalité. Cependant, le taux de détection et de prévention par les forces de l'ordre est très basique. Ce chapitre tente d'examiner le cadre juridique, réglementaire et de supervision ainsi que les défis sous-jacents aux mesures d'application et de contrôle dans les économies d'Afrique de l'Ouest. Il met également en lumière l'état d'avancement de la mise en œuvre par les pays des instruments internationaux existants sur la cybercriminalité, conformément aux normes du GAFI sous la recommandation 36 qui invite les pays à ratifier d'autres conventions internationales pertinentes.

Cadre juridique, réglementaire et d'application pour la cybersécurité et la cybercriminalité en Afrique de l'Ouest

45. Il existe d'importantes lacunes législatives dans certains pays, notamment en ce qui concerne les pouvoirs de l'autorité centrale chargée de la lutte contre la cybercriminalité et les cadres juridiques et d'application des pays pour détecter, prouver et freiner efficacement le blanchiment de capitaux ou le financement du terrorisme associés à la cybercriminalité. Alors que les cadres juridique et répressif prévoient des mesures d'application de la loi pour enquêter sur les cybercriminels et les poursuivre, le cadre réglementaire dans la plupart des pays d'Afrique de l'Ouest prévoit des mesures préventives qui dans l'ensemble sont soit insuffisantes, soit faibles. Bien que quelques pays aient réalisé des progrès en matière d'obtention de preuves électroniques et numériques au cours des enquêtes, cela reste un défi dans plusieurs autres pays..

46. Il faut noter que la législation pénale existante et les normes anti-blanchiment du GAFI sont également applicables contre la cybercriminalité et peut être utile aux autorités compétentes. Il s'agit notamment de déterminer comment les catégories d'infractions existantes (au titre de la R.3) sont applicables, ainsi que les mesures préventives/le cadre réglementaire existant pour les IF, les EPNFD et les PSAV. Par exemple, dans de nombreuses études de cas du chapitre 3, il est très clair que les catégories d'infractions existantes, telles que la fraude, le vol, l'extorsion, la falsification, l'exploitation sexuelle, etc. sont applicables dans le cyberespace.

47. La reconnaissance de l'applicabilité des outils et normes existants est importante, car elle montre que les autorités compétentes peuvent agir le cas échéant, en attendant la promulgation de nouvelles lois et réglementations. Cette reconnaissance est également importante pour encourager la collaboration transfrontalière, en particulier pour lever les obstacles de la double incrimination.

48. Le tableau ci-dessous présente les lois, règlements, directives et orientations en matière de cybersécurité, de cybercriminalité, de protection des données et de lutte contre le blanchiment de capitaux et le financement du terrorisme, tels qu'ils ont été fournis par les experts des États membres.

Tableau 3.1 : Cybersécurité / cybercriminalité, lois, règlements et directives en Afrique de l'Ouest

États membres	Lois et dispositions réglementaires	Commentaires
Bénin	La loi n° 2017-20 du 20 avril 2018 portant code du numérique ; la loi n° 2018-16 du 28 décembre 2018 portant code pénal au Bénin en ses articles 161 relatif aux actes de terrorisme, 162-3 relatif à l'informatique, 670 à 689 relatif aux infractions cybernétiques, informatiques ; la loi n° 2012-15 du 18 mars 2013 portant code de procédure pénale ; la loi n° 2011-20 du 12 octobre 2011 relative à la lutte contre la corruption et autres infractions connexes ;	Le Bénin dispose d'un Code numérique qui réprime la cybercriminalité et les conséquences qu'elle peut entraîner lorsque ses auteurs utilisent ou non des méthodes pour dissimuler l'origine criminelle de leurs revenus. Le Code pénal dans toutes ses dispositions prévoit les peines prévues pour sanctionner les infractions de blanchiment de capitaux et de financement du terrorisme liées à la cybercriminalité. La loi sur la lutte contre la corruption et autres infractions connexes sanctionne les infractions de financement des capitaux, le financement du terrorisme lié à la cybercriminalité.
Burkina Faso	Loi n° 001-2021/AN du 30 mars 2021 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel ; Loi n° 040-2019/AN du 29 mai 2019 portant code de procédure pénale ; Loi n° 005-2017/AN du 19 janvier 2017 portant création, organisation et fonctionnement des pôles judiciaires spécialisés dans la répression des infractions économiques et financières et de la criminalité organisée ; Loi n° 016-2016/AN du 3 mai 2016 relative à la lutte contre le blanchiment des capitaux et le financement du terrorisme ; Loi n° 061-2008/AN du 27 novembre 2008 portant réglementation générale des réseaux de communications électroniques ; Décret n° 2020-0099/PRES/PM/MSECU/MJ/ MINEFID du 14 février 2020 portant création d'un réseau de communications électroniques. 061-2008/AN du 27 novembre 2008 portant réglementation générale des réseaux et services de communications électroniques ; Décret n° 2020-0099/PRES/PM/MSECU/MJ/ MINEFID du 14 février 2020 portant création, attributions, organisation et fonctionnement de la Brigade Centrale de Lutte contre la Cybercriminalité ; Décret n° 2013-149/PRES/PM/MJ/ MINEFID du 14 février 2020 portant création, attributions, organisation et fonctionnement de la Brigade Centrale de Lutte contre la Cybercriminalité. 2013-149/PRES/PM/MDENP/MEF/MJ du 21 mars 2013 définissant les obligations des opérateurs de services de communications électroniques en matière de conservation des données de trafic et de localisation ; Décret n° 2013-1053/PRES/PM/MEF/MATS du 11 novembre 2013 portant création de l'Agence nationale de la sécurité des systèmes d'information.	La lutte contre la cybercriminalité a fait l'objet d'une série de textes tendant à l'encadrer. En termes de textes législatifs et réglementaires, on note l'adoption d'un certain nombre de textes qui réglementent et répriment les infractions de cybercriminalité.

États membres	Lois et dispositions réglementaires	Commentaires
Cabo Verde	Le décret-loi nº 9/2021 du 29 janvier a créé le régime juridique de la cybersécurité et l'équipe d'intervention en cas d'incident de sécurité informatique ; création de la loi sur la cybercriminalité nº 8/IX/2017 du 20 mars - relative à la coopération internationale en matière pénale et à la collecte de preuves sous forme électronique ; régime général de protection des données par la loi nº 41/VIII/2013 du 17 septembre ; loi sur le commerce électronique ; loi sur l'infrastructure à clé publique ; loi sur la signature numérique ; loi sur l'identité électronique.	Le Cabo Verde établit les dispositions pénales, matérielles et procédurales, ainsi que les dispositions relatives à la coopération internationale en matière pénale, concernant la lutte contre la cybercriminalité et la collecte de preuves numériques et de données électroniques.
Côte d'Ivoire	La loi n° 2013-451 du 19 juin 2013 relative à la lutte contre la cybercriminalité ; la loi n° 2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel ; la loi n° 2011-546 du 30 juillet 2013 relative aux transactions électroniques régissant le commerce électronique, la publicité, etc. ; l'ordonnance n° 2012-243 régissant toutes les activités liées aux TIC à partir ou à destination de la Côte d'Ivoire ; et le décret n° 2011-476 du 21 décembre 2011 portant identification des abonnés des fournisseurs de services de télécommunications.	Cette loi définit des infractions spécifiques liées aux TIC, aux violations de la propriété intellectuelle, aux actes illégaux sur les réseaux de communication électronique et aux responsabilités des fournisseurs de services en ligne. Elle adapte les infractions traditionnelles aux TIC et clarifie la procédure pénale en matière de cybercriminalité. Outre cette loi, d'autres lois, règlements et décrets ont été publiés, en plus du code pénal, par les autorités ivoiriennes dans le but de réglementer et de sécuriser le cyberespace ivoirien.
Gambie	Loi sur l'information et les communications (ICA), 2009 ; loi sur les preuves, 1994 ; loi sur le droit d'auteur, 2004 ; projet de loi sur les infractions pénales, 2020 ; code pénal (1933, modifié en dernier lieu par la loi n° 18 de 2010) ; Code de procédure pénale (1933, modifié en dernier lieu par la loi n° 5 de 2005) ; et	Le Conseil de l'Europe et OCWAR-C ont soutenu le ministère gambien de la Justice et le ministère de la Communication et de l'économie numérique dans la préparation d'un projet de loi sur la cybercriminalité, qui a été finalisé en décembre 2019 et ouvert à la consultation publique jusqu'en janvier 2020. Le ministre de la communication et de l'économie numérique travaille toujours à la finalisation du projet de loi sur la cybercriminalité.
Ghana	Cyber Security Act, 2020 (Act 1038) ; National Information Technology Agency Act (NITA), 2008 (Act 771) ; Electronic Transactions Act, 2008 (Act 772) ; Electronic Communications Act, 2008 (Act 775) ; Data Protection Act, 2012 (Act 843) ; Economic and Organized Crime Office Act, 2010 (Act 807) ; Anti-Money Laundering Act, 2020 (Act1044) ; Anti-Terrorism Act, 2008 (Act 762) ; Payment Systems and Services Act 2019 (Act 987) ; Mutual Legal Assistance Act, 2010 (Act 807) ; Banks and Specialised Deposit-Taking Institutions Act 2016 (Act 930) ; Non-Bank Financial Institution Act 2008 (Act 774).	La loi sur la cybersécurité vise à promouvoir le développement de la cybersécurité et à régler les questions connexes. Elle a également créé l'Autorité de la cybersécurité (CSA) pour réglementer les activités de cybersécurité. Le conseil d'administration de l'autorité est constitué par les ministres de la communication, de la défense, de la sécurité nationale et de l'intérieur. Pour assurer une bonne coordination en cas d'incidents liés à la cybersécurité, l'autorité est tenue de mettre en place des équipes sectorielles d'intervention en cas d'urgence informatique (CERT), notamment pour le secteur bancaire et financier.

États membres	Lois et dispositions réglementaires	Commentaires
Guinée	Loi L/037/AN/2016 relative à la cybersécurité et à la protection des données personnelles ; Loi L/035/AN/2016 relative aux transactions électroniques ; Loi n° 059/AN/2016 portant code pénal ; Loi L/2021/024/AN du 17 août 2021 relative à la lutte contre le blanchiment de capitaux et le financement du terrorisme.	Les lois définissent les règles et les mécanismes pour lutter contre la cybercriminalité et ainsi créer un environnement favorable, propice et sécurisé dans le cyberespace, mais aussi pour permettre à la République de Guinée de se conformer à ses engagements communautaires et internationaux en matière de cybersécurité. Elle favorise également la modernisation de l'utilisation des TIC ainsi que le soutien à la lutte contre le blanchiment de capitaux et le financement du terrorisme.
Libéria	Fraud Act, 2012 - criminalise la fraude électronique et la fraude postale. AML/CFT Preventive Measure for Proceeds of Crimes Act 2021 (loi sur les mesures préventives de lutte contre le blanchiment de capitaux et le financement du terrorisme pour les produits du crime) - reconnaît la fraude comme une infraction préalable à la lutte contre le blanchiment de capitaux. Telecommunications Act 2007 (loi sur les télécommunications) - permet aux services répressifs d'obtenir des preuves numériques.	Le Liberia n'a pas de législation directe sur la cybercriminalité. Un projet de loi (Cybercrime Act) a été soumis au Parlement en vue de sa promulgation. Toutefois, le Liberia s'appuie sur d'autres textes législatifs pour traiter les questions relatives à la cybercriminalité.
Nigéria	Cybercrime (Prohibition, Prevention, etc.) Act, 2015 ; Economic and Financial Crimes Commission (Establishment) Act, 2004 ; Advanced Fee Fraud and Other Related Offenses Act, 52 (2006) ; Money Laundering (Prohibition) Act, 2011 as amended in 2013 ; the Nigerian Evidence Act, The Criminal Code Act, The Penal Code Act, The Terrorism (Prevention) Act, 2013, and the National Identity Management Commission Act, 2007.	Avec l'avènement de la loi sur la cybercriminalité en 2015, le Nigéria est devenu plus équipé juridiquement dans la lutte contre les activités cybercriminelles. Toutefois, il n'est peut-être pas approprié de discuter de la loi sur la cybercriminalité de 2015 sans faire la lumière sur les lois habilitantes qui existaient pour contrôler la cybercriminalité (c'est-à-dire la loi sur l'EFCC, la loi sur l'AFF, etc) avant que la loi ne soit promulguée.
Sénégal	Loi 2008-08 relative aux transactions électroniques et à la promotion du commerce des TIC ; loi 2008-12 du 25 janvier 2008 relative à la protection des données personnelles ; loi 2008-11 du 25 janvier 2008 relative à la cybercriminalité ;	Dès 2008, le pays a adopté un cadre normatif pour lutter contre la cybercriminalité et réguler le système d'information. Ces lois encadrent les transactions électroniques, le traitement des données, favorisent le développement du commerce dans le secteur des TIC et la protection des données personnelles, ainsi que le respect des libertés et des droits fondamentaux de l'homme.
Sierra Leone	La loi sur les télécommunications de 2006 ; la loi sur la cybersécurité et la cybercriminalité de 2021 ; la loi sur la lutte contre le blanchiment de capitaux et le financement du terrorisme de 2012 ; la loi sur la sécurité nationale et le renseignement central de 2002.	Cette loi fournit un cadre pour lutter contre la cybercriminalité, le blanchiment de capitaux et le financement du terrorisme, protéger les structures d'information et les systèmes informatiques nationaux essentiels, collecter des preuves électroniques pour enquêter sur la cybercriminalité et engager des poursuites, protéger la sécurité nationale, mener des opérations secrètes de renseignement sur l'ensemble du territoire de la Sierra Leone, et faciliter la coopération internationale.

49. Le tableau 3.1 présente les dispositions légales et réglementaires mises en place par les autorités compétentes des États membres pour lutter contre la cybercriminalité. À l'exception de quelques-uns qui s'appuient encore sur d'autres lois connexes pour lutter contre la cybercriminalité, la plupart des États membres disposent de lois autonomes sur la cybersécurité et la cybercriminalité. L'application de ces lois à la détection, aux enquêtes et aux poursuites s'est principalement concentrée sur l'infraction principale, ignorant la nécessité d'une détection et d'une enquête parallèles sur l'aspect blanchiment de capitaux des affaires.

Institutions chargées de la lutte contre la cybercriminalité en Afrique de l'Ouest

Bénin

50. Le chef de file de la lutte contre la cybercriminalité est l'Office central de répression de la cybercriminalité (OCRC), placé sous l'autorité du directeur de la police judiciaire, qui est chargé de veiller à ce que toutes les mesures préventives soient prises en compte dans la lutte contre la cybercriminalité, y compris les infractions relatives aux systèmes informatiques, ainsi qu'à la gestion des bases de données. Elle fournit également une assistance technique aux services qui requièrent son expertise, organise des formations, etc. Les autres institutions chargées de la lutte contre la cybercriminalité sont le Ministère de l'Economie et des Finances, le Ministère de la Justice, le Ministère de l'Intérieur et de la Sécurité Publique, l'Agence Nationale d'Identification des Personnes (ANIP), l'Agence des Systèmes d'Information et du Numérique, l'Agence du Développement Numérique (ADN), et l'Agence Béninoise de Communications Electroniques Universelles et des Postes (ABSUCEP).

Burkina Faso

51. Le Ministère de la Transition Numérique, des Postes et des Communications Electroniques (MTDPCE) assure la mise en œuvre et le suivi de la politique gouvernementale en matière de développement de l'économie numérique, des postes et de la transformation numérique. L'Agence nationale du renseignement a pour principales missions de collecter et d'exploiter les informations reconnues d'intérêt vital pour la sécurité. La Commission de l'informatique et des libertés (CIL) est l'autorité de contrôle chargée de veiller à la protection des données à caractère personnel, en informant toutes les personnes concernées et les responsables de traitement de leurs droits et obligations et en contrôlant l'utilisation des technologies de l'information et de la communication appliquées au traitement des données à caractère personnel. L'Agence nationale de la sécurité des systèmes d'information (ANSSI) est chargée de gérer la sécurité des systèmes d'information et du cyberespace. L'Autorité de régulation des communications électroniques et des postes (ARCEP) est chargée de veiller au respect de la réglementation en vigueur dans le secteur des communications électroniques, de gérer et d'attribuer les fréquences radioélectriques et d'en contrôler les conditions d'utilisation, de suivre l'évolution des technologies et de prescrire les mesures propres à stimuler et à faciliter l'investissement dans le secteur des communications électroniques. La Cellule nationale de traitement des informations financières (CENTIF) est chargée de la collecte, du traitement et de la diffusion des informations aux autorités compétentes ou à d'autres cellules de renseignement financier. Les autres acteurs étatiques sont la Direction générale de la police nationale ; l'État-major général de la gendarmerie nationale ; la Direction générale des transmissions et de l'informatique ; la Brigade centrale de lutte contre la cybercriminalité ; la Brigade spéciale d'enquêtes antiterroristes et de lutte contre la criminalité organisée ; l'Office de l'identification nationale ; et le ministère de la Justice.

Cabo Verde

52. Le Cap-Vert continue d'investir massivement dans une société de la connaissance, de l'information, de l'innovation et de la prospérité, ainsi que dans l'investissement et le renforcement des institutions TIC, à savoir l'Agence de régulation multisectorielle de l'économie, le ministère de l'économie numérique, le Conseil national pour le développement des TIC et la Commission nationale pour la protection des données, et dans la fourniture d'in-

frastructures technologiques de qualité, ainsi que dans la formation des ressources humaines. Le gouvernement a approuvé la stratégie nationale de cybersécurité (ENCS) et créé le noyau national de cybersécurité (NNCS). Le gouvernement a également mis en place l'Équipe d'intervention en cas d'urgence informatique et la Brigade centrale de lutte contre la cybercriminalité et le terrorisme de la police judiciaire (BCCCT) en 2021.

Côte d'Ivoire

53. Les acteurs étatiques qui sont en première ligne dans la lutte contre la cybercriminalité sont la Direction du traçage informatique (DITT) est une entité de la police nationale dotée de services spécialisés responsables des infrastructures de télécommunications et fournissant une assistance technique aux services répressifs et judiciaires. Cette structure a été créée en mai 2007 dans le cadre de la lutte contre la cybercriminalité. Le Computer Emergency Response Team (CI-CERT) est mis en place par l'Autorité de régulation des télécommunications en juin 2009. Il s'agit d'un centre d'alerte et de réponse aux cyberattaques survenant dans le cyberespace ivoirien. Dotée de ressources humaines spécialisées dans les systèmes de sécurité de l'information, l'équipe offre une assistance technique proactive et réactive aux entreprises et aux particuliers lors de failles de sécurité. En tant que centre de coordination avec un réseau de partenaires mondiaux, elle est le point focal national pour la surveillance de la sécurité informatique, la détection et l'alerte en cas d'incident de sécurité. Le forum sur la lutte contre la cybercriminalité est également une convention de partenariat signée en 2011 et actualisée en 2014, entre la Direction générale de la police nationale et le CI-CERT. Il s'agit d'une entité intégrée à la DITT de la Police Nationale, qui en assure la gestion. La PLCC est une autre structure en charge de la lutte contre la cybercriminalité en Côte d'Ivoire et est appuyée dans l'exécution de ses missions, par le CI-CERT et le Computer Forensic Lab de la DITT. En plus des enquêtes criminelles qui couvrent la recherche et l'administration de la justice pour les cybercriminels présumés.

54. Les autres acteurs étatiques de la lutte contre la cybercriminalité sont la CRF, l'Agence de gestion et de recouvrement des avoirs criminels (AGRAC), la Direction de la police économique et financière, l'Unité de lutte contre la criminalité économique et financière, qui est un tribunal pénal de première instance spécialisé dans la criminalité économique et financière, le ministère public, la Direction de la police criminelle et les sections de recherche de la Gendarmerie nationale. Les acteurs non étatiques sont les entreprises de télécommunication, les opérateurs de téléphonie mobile, les fournisseurs d'accès à Internet et les institutions financières.

Gambie

55. Le ministère des communications et de l'économie numérique supervise l'élaboration et la mise en œuvre des lois, des règlements et de la stratégie pour le secteur des TIC. Le secteur des télécommunications, un élément clé de l'infrastructure nationale critique de la Gambie, est largement réglementé par l'Autorité de régulation des services publics (Public Utilities Regulatory Authority - PURA). La PURA met en place l'équipe de sécurité informatique et de réponse aux incidents de la Gambie (gmCSIRT). La gmCSIRT soutient tous les détenteurs d'infrastructures d'information critiques (CII) en Gambie. Le cabinet du procureur général et le ministère de la justice, par l'intermédiaire du département des poursuites pénales, sont chargés d'engager, de reprendre, de poursuivre ou d'interrompre les procédures pénales à l'encontre de tout auteur d'infraction. Le pouvoir judiciaire de la Gambie est chargé de trancher les litiges dans le respect de la légalité, d'administrer les tribunaux, les registres, les procédures, les directives et les procédures et d'appliquer les décisions, les ordonnances, les jugements et les arrêts. La police gambienne est également en première ligne dans la lutte contre la cybercriminalité. Dans le cadre du projet OWAR C, la police a bénéficié d›un laboratoire numérique équipé et 15 officiers de police ont été formés à la conduite d›enquêtes criminalistiques numériques sur les appareils électroniques et les réseaux afin de pouvoir mener à bien des enquêtes sur la cybercriminalité. La CRF est chargée d›analyser, de diffuser ou de classer les déclarations de transactions suspectes (DTS), de rechercher des informations ou d›y répondre. La Gambie a créé une alliance pour la cybersécurité (GCSA) en 2017 et a élaboré un plan national de cybersécurité (2020-2024) qui sert de guide pour protéger les systèmes d›information du pays, les infrastructures critiques et le cyberespace de la Gambie en général.

Ghana

56. Les acteurs publics responsables de la lutte contre la cybercriminalité au Ghana sont le Centre de renseignement financier (FIC), l'Unité de lutte contre la cybercriminalité du Département des enquêtes criminelles du Service de police du Ghana, l'Office de lutte contre la criminalité économique et organisée (EOCO), la National Cyber Authority, le National Intelligence Bureau (NIB), la National Communications Authority (NCA), la Bank of Ghana (BoG), et la Securities and Exchange Commission (SEC). Le ministère des communications et de la numérisation (MOCD), utilisant la carte du Ghana comme document de référence, a annoncé le réenregistrement des cartes SIM (Subscriber Identification Module) proposées par les entreprises de télécommunications du pays. Le Centre national de cybersécurité du MOCD est chargé du renforcement des capacités et de la sensibilisation du grand public à la cyberhygiène et à la cybersécurité.

Libéria

57. L'Autorité des télécommunications du Liberia (LTA) est chargée d'octroyer des licences et de réglementer les opérateurs de télécommunications, les fournisseurs de services et de contrôler leurs performances. et de réglementer les opérateurs de télécommunications, les fournisseurs de services et de contrôler leurs performances, de mettre en œuvre des politiques et des stratégies en matière de services de télécommunications et de fournir un programme politique pour le développement des TIC et des télécommunications au Libéria. L'Agence nationale de sécurité (NSA) dispose d'un laboratoire de lutte contre la cybercriminalité, mais les lignes directrices en matière de signalement et d'accessibilité au public pour signaler les cas de cybercriminalité ne sont pas connues. La police nationale du Liberia (LNP) dispose d'une section chargée de traiter les affaires de cybercriminalité, mais elle est inactive en raison de la faiblesse de ses effectifs et de son manque de connaissances et d'outils en matière de cybercriminalité. L'agence de renseignement financier (FIA) est l'agence centrale nationale chargée de recevoir et d'analyser les rapports de transactions ou d'activités suspectes. L'Agence libérienne de prévention et d'atténuation de la cybercriminalité (LCCPMA), en tant qu'institution, dispose également de vastes réseaux de soutien internationaux, dont certains comprennent un partenariat avec la Global Cyber Alliance en 2020, et avec le Global Forum on Cyber Expertise (GFCE) en 2021, etc.

Nigéria

58. Les cadres institutionnels examinés sont la Nigerian Financial Intelligence Unit (NFIU), la Special Control Unit against Money Laundering (unité spéciale de contrôle contre le blanchiment de capitaux) et le Nigerian Cyber Crime Working Group (groupe de travail nigérian sur la cybercriminalité). La cybercriminalité est un terme qui décrit de manière générale les activités criminelles dans lesquelles les ordinateurs ou les réseaux informatiques sont un outil, une cible ou un lieu d'activité criminelle. Avec l'accès facile à l'internet, la cybercriminalité est devenue de plus en plus répandue parmi les jeunes d'aujourd'hui. Ce qui est encore plus inquiétant, c'est la vitesse à laquelle les victimes tombent dans le panneau. Ce qui est encore plus inquiétant, c'est que ces jeunes sont passés maîtres dans l'art de la cybercriminalité.

Sénégal

59. Afin de contenir les impacts de la cybercriminalité et de questionner les cadres et les outils nécessaires à la compréhension de l'environnement numérique, le Sénégal a mis en place en 2018 une école nationale de cybersécurité à vocation régionale. Cette école vise principalement à assurer la formation d'experts en cybersécurité et à constituer un pôle de référence en Afrique. Enfin, pour adapter leurs organisations et se donner les moyens de répondre efficacement au défi sécuritaire posé par la cybercriminalité, la Police et la Gendarmerie nationales ont mis en place des services spécialisés dans la lutte contre la cybercriminalité. Il s'agit respectivement de la Division spéciale de cybersécurité (DSC) et de la Plateforme numérique de lutte contre la cybercriminalité (PNLC).

Guinée

60. L'Agence nationale de la sécurité des systèmes d'information (ANSSI) est un acteur majeur de la cybersécurité et fournit une expertise et une assistance technique aux régulateurs, aux forces de l'ordre et aux entreprises. Elle fournit un service de surveillance, de détection, d'alerte et de réaction aux cyber-attaques. L'unité de lutte contre la cybercriminalité de la direction centrale de la police judiciaire est également un organe créé par le ministre de la sécurité et de la protection civile et joue un rôle très important dans la lutte contre la cybercriminalité. La division des enquêtes criminelles de la direction centrale de la police judiciaire est également responsable des enquêtes sur la cybercriminalité et travaille en étroite collaboration avec tous les procureurs du pays. Les autres acteurs étatiques sont l'autorité de régulation des postes et télécommunications, l'Agence nationale de lutte contre la corruption et de promotion de la bonne gouvernance (ANLC), l'unité d'intelligence financière, le réseau central d'INTERPOL (NCB) et le bureau des procureurs.

Sierra Leone

61. L'unité de lutte contre la cybercriminalité enquête sur tous les cas de cybercriminalité signalés. La Commission nationale des télécommunications (NATCOM) est le principal régulateur de tous les services de téléphonie mobile et des fournisseurs d'accès à Internet (FAI). Elle émet des directives et des lignes directrices et collabore avec les enquêteurs en cybercriminalité et la CRF. La CRF fournit des analyses financières et des rapports de renseignement financier sur les activités de blanchiment de capitaux et de financement du terrorisme, le cas échéant. Les autres acteurs étatiques sont l'Autorité nationale d'enregistrement civil (NCRA), l'Unité de lutte contre la criminalité transnationale organisée (TOCU), l'Unité centrale de renseignement et de sécurité (CISU), la police sierra-léonaise et le Directeur des poursuites publiques (DPP). Outre ces acteurs étatiques, il existe des initiatives de collaboration interinstitutionnelle telles que le Conseil consultatif national sur la cybersécurité, le Groupe de travail technique national sur la cybersécurité, le Groupe de travail sur la criminalité financière et le Comité conjoint sur le renseignement. Ces organes sont composés d'acteurs issus des services répressifs, des organismes de réglementation, des institutions chargées de la sécurité et de la collecte de renseignements, ainsi que des ministères compétents. L'objectif principal de ces structures interagences est d'atteindre un niveau élevé de coopération et de collaboration afin de garantir un environnement cybernétique sûr. La Sierra Leone a également élaboré une stratégie nationale de cybersécurité et de protection des données (2017 - 2022). La stratégie classe la cybercriminalité en crimes cyberdépendants (crimes commis avec l'utilisation d'appareils TIC uniquement, où les appareils sont à la fois l'outil pour commettre le crime et la cible du crime, tandis que les crimes cyber-compatibles traitent des crimes traditionnels qui, en raison de l'utilisation d'appareils TIC et de réseaux, ont pris de l'ampleur ou de la portée.

Ratification d'instruments internationaux

62. Conformément aux exigences des normes mondiales, en particulier la recommandation 36 du GAFI sur la coopération internationale (c'est-à-dire la mise en œuvre d'instruments internationaux), «*les pays .... sont également encouragés à ratifier et à mettre en œuvre d'autres conventions internationales pertinentes, telles que la Convention du Conseil de l'Europe sur la cybercriminalité, 2001 ; ....*». Cette exigence est connue sous le nom de «Convention de Budapest».

63. Comme la Convention de Budapest, la Convention de l'Union africaine sur la cybersécurité et la protection des données personnelles (juin 2014), connue sous le nom de Convention de Malabo, encourage ses membres qu'ils ratifient et mettent en œuvre les dispositions énoncées dans la convention et convenues par les membres. Cependant, les mécanismes de coopération interinstitutionnelle et internationale sont faiblement réglementés par la législation, de sorte que les défis en matière d'enquêtes et de poursuites pénales dans ce domaine restent importants dans certains pays. Même si presque tous les pays d'Afrique de l'Ouest ont mis en place une stratégie nationale de lutte contre la cybercriminalité, certains pays doivent encore ratifier les conventions de Budapest et de Malabo dans la perspective de renforcer la coopération régionale transfrontalière.

64. Vous trouverez ci-dessous l'état d'avancement de la ratification et de la mise en œuvre des deux instruments complémentaires (conventions) destinés à aider les États membres à renforcer leur cadre de prévention et de répression de la cybercriminalité.

Figure 3.1 : Ratification d'instruments internationaux

BUDAPEST	MALABO
Cabo Verde Senegal Ghana Nigeria	Cabo Verde Cote d'Ivoire Ghana Guinea, Niger Senegal Togo
Signatories and Invited to Accede Benin Burkina Faso Cote D'Ivoire Niger Sierra Leone	**Signed but yet to Ratify** Comoros Gambia Ghana Guinea Bissau Sierra Leone Sao Tome & Principe Togo

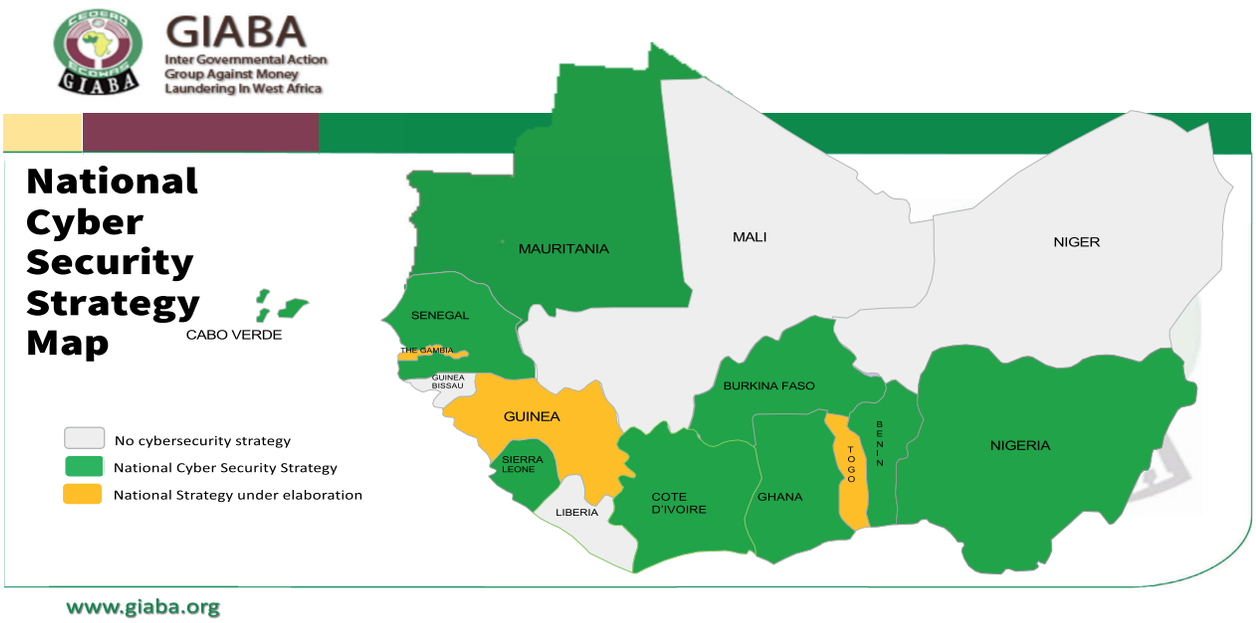
Source : OCWAR-C

65. La figure 3.1 ci-dessus montre que 4 pays, le Cabo Verde, le Ghana, le Nigeria et le Sénégal étaient parties à la Convention de Budapest, tandis que 5 autres pays, le Bénin, le Burkina Faso, la Côte d'Ivoire, le Niger et la Sierra Leone sont maintenant signataires et invités à adhérer à la convention, ce qui porte à 9 le nombre de pays d'Afrique de l'Ouest qui ont pris des mesures pour mettre en œuvre la Convention de Budapest sur la cybercriminalité. Dans le cas de la convention de Malabo, seuls le Ghana et le Togo ont pleinement mis en œuvre l'exigence (signature et ratification) de la convention en Afrique de l'Ouest. Outre le Ghana et le Togo, cinq autres pays ont seulement ratifié (Cabo Verde, Côte d'Ivoire, Guinée, Niger et Sénégal) sans signer la convention, tandis que trois autres pays l'ont signée (Gambie, Guinée-Bissau et Sierra Leone) sans la ratifier. Il y a cependant deux autres États membres du GIABA non membres de la CEDEAO qui ont signé la convention de Malabo mais qui ne l'ont pas encore ratifiée.

66. Par ailleurs, le projet de l'Union européenne sur la criminalité organisée : Réponse de l'Afrique de l'Ouest à la cybersécurité et lutte contre la cybercriminalité (OCWAR-C) exécuté par le groupe Expertise France a travaillé avec les États membres pour développer des stratégies nationales de cybersécurité. Au cours de la période examinée, 8 pays ont mis en place des stratégies nationales et 3 autres sont en cours de finalisation, ce qui porte le total à 11 pays sur 15. Les quatre autres pays qui n'ont pas encore élaboré leur stratégie nationale de cybersécurité sont la Guinée-Bissau, le Liberia, le Mali et le Niger. La carte ci-dessous montre l'état d'avancement des stratégies nationales.

67. Au niveau régional, la CEDEAO a publié une directive (2010) sur la lutte contre la cybercriminalité et l'adoption d'un droit pénal substantiel et d'une procédure pour lutter contre la cybercriminalité dans les États membres. Outre la directive, la CEDEAO a mis en œuvre les dispositions d'harmonisation, en particulier l'Acte additionnel sur la protection des données personnelles et la garantie de la confidentialité, et l'Acte additionnel sur les transactions électroniques avec les conditions d'acceptation de la signature électronique.

Figure 3.2 : Stratégie nationale de cybersécurité en Afrique de l'Ouest



Source : OCWAR-C

Défis juridiques, réglementaires et d'application

68. La région de l'Afrique de l'Ouest a fourni des efforts et des progrès considérables dans la lutte contre la cybercriminalité, ainsi que contre d'autres infractions sous-jacentes. Mais ces efforts et ces progrès n'ont pas été exempts de défis, qui restent redoutables et persistants, car les criminels utilisent de nouvelles méthodes et techniques pour éviter d'être détectés. Voici un résumé de ces défis.

69. Même si la plupart des États membres du GIABA ont pris des mesures pour se doter de lois permettant aux autorités compétentes de lutter contre la cybercriminalité, le cadre juridique et institutionnel existant présente encore des limites. Il existe des zones d'ombre qui doivent être explicitées là où les lois existent et les pays qui n'ont pas de lois autonomes devraient accélérer le processus pour en promulguer une. Les lois devraient s'inspirer des dispositions des conventions de Budapest et de Malabo, notamment en ce qui concerne l'acceptation des preuves numériques et électroniques dans la procédure judiciaire et l'accélération de la procédure judiciaire. Les normes du GAFI ont également prévu diverses recommandations (en particulier la recommandation R.3 et d'autres recommandations traitant des mesures préventives pour les IF, les EPNFD et les PSAV).

70. Faible niveau d'opérationnalité des structures et mécanismes chargés de la cybersécurité et de la lutte contre la cybercriminalité. La mise en place d'un laboratoire numérique, équipé d'outils performants pour analyser les preuves numériques, et l'utilisation efficace de ces technologies tout au long de la chaîne pénale doivent être renforcées. Les rôles et responsabilités des différentes parties prenantes doivent être clairement définis et les modalités de collaboration et de coordination comprises.

71. L'expertise et les connaissances des autorités compétentes en matière de lutte contre la cybercriminalité dans les enquêtes financières et numériques sont encore très limitées et nécessitent une formation continue de ces acteurs (police, procureurs, ingénieurs en TIC, analystes de la CRF, magistrats et tous les acteurs de la chaîne pénale).

72. L'insuffisance des ressources (financières et matérielles) continue de ralentir la lutte contre la cybercriminalité, car les cas sont souvent signalés en nombre et les documents à analyser sont souvent volumineux et nécessitent à la fois des compétences et de la main-d'œuvre. Par exemple, lorsque des millions d'enregistrements, de comptes, de cartes de crédit ou de photos personnelles sont piratés, il faut un grand nombre de personnes hautement qualifiées pour mener à bien l'enquête en temps voulu.

73. Manque de sensibilisation aux dangers du manque de précaution et de l'utilisation inappropriée du cyberespace, y compris des médias sociaux. Les utilisateurs des TIC et les victimes de cybercrimes ne sont pas suffisamment conscients de leur droit à porter plainte. En outre, les cybercriminels sont enhardis par le fait que la plupart des victimes, en particulier lorsqu'il s'agit de certains délits portant atteinte à l'honneur et à la dignité, s'abstiennent de porter plainte et préfèrent se résigner à leur sort afin d'éviter tout scandale ou stigmatisation.

74. Le manque de collaboration interinstitutionnelle et de coopération internationale. La ratification des conventions de Budapest et de Malabo sur la cybercriminalité est encore très faible, tout comme les avantages qui en découlent en termes de coopération internationale et de renforcement des capacités. L'intensification de la coopération inter-agences pour une meilleure gestion des informations et des renseignements qui peuvent conduire à la détection des infractions, à l'arrestation des auteurs présumés et à leur transmission aux bureaux des procureurs compétents.

75. La nature complexe de l'enquête nécessaire à la collecte de preuves pour poursuivre les cyber-attaques constitue un obstacle majeur. La principale difficulté rencontrée par les services répressifs est de remonter à la source principale de la cyber-attaque. L'unité de lutte contre la cybercriminalité et les autres unités chargées de l'application de la loi sont souvent incapables d'atteindre la source de l'information, même à l'intérieur du pays, et la situation est encore plus complexe lorsque la cyberattaque émane de l'étranger et qu'il est nécessaire de recourir à une demande d'entraide judiciaire.

CHAPITRE 6

CONCLUSION ET RECOMMANDATIONS

Conclusion

76. L'innovation et les technologies émergentes ont changé la façon dont les entreprises sont menées à travers le monde. Dans le même ordre d'idées, les organisations et les institutions ont adopté des méthodes intelligentes pour mettre en œuvre des programmes qui conduisent à l'efficience et à l'efficacité. Le monde a connu une croissance significative grâce à l'utilisation de ces technologies émergentes, qu'il s'agisse de technologies financières, d'intelligence artificielle, d'intelligence économique, de robotique, de ChatGPT, etc.

77. Toutefois, ces technologies, qui opèrent sur les autoroutes de l'internet connues sous le nom de cyberespace, sont utilisées pour commettre, faciliter et rendre possible des infractions classiques (infractions principales au blanchiment de capitaux et au financement du terrorisme). La cybercriminalité et le blanchiment de capitaux et le financement du terrorisme sont inextricablement liés et posent ensemble des problèmes de sécurité majeurs dans le monde entier. En règle générale, un niveau élevé de compétences en matière de TIC est nécessaire pour commettre des actes de cybercriminalité et pour les contrer. Ce n'est toutefois pas le cas en Afrique de l'Ouest, où l'on constate un décalage entre les compétences supérieures démontrées par les cybercriminels et celles des autorités compétentes qui luttent contre la cybercriminalité.

78. Bien qu'il existe un large éventail de méthodes et de techniques utilisées par les cybercriminels pour blanchir le produit de leurs activités criminelles, les enquêteurs et les procureurs n'ont mené que peu ou pas d'enquêtes financières parallèles lorsque la cybercriminalité est détectée. Ils sont également confrontés dans de nombreux cas à la difficulté d'établir la preuve de l'infraction de cybercriminalité, en raison du manque de technologie ou d'équipement requis, de l'inefficacité de la coordination nationale intégrée entre les unités opérationnelles de lutte contre le blanchiment de capitaux et le financement du terrorisme, et de l'absence de mise en œuvre des mécanismes de coopération régionale et internationale.

Recommandations

79. Afin de maintenir le cap dans la lutte contre la cybercriminalité en Afrique de l'Ouest tout en la rendant plus efficace et plus dissuasive, les recommandations suivantes sont formulées à l'intention du public et des autorités compétentes qui luttent contre la cybercriminalité.

Pour le public

80. Lancer et intensifier des campagnes de sensibilisation du grand public sur le mode opératoire des cybercriminels et les risques liés à l'utilisation de l'internet, ainsi que sur les méthodes et techniques existantes déployées par les cybercriminels.

81. Promouvoir la culture de la cybersécurité dans la région et aider les pays à mettre en place un cadre juridique et institutionnel conforme aux normes internationales en vigueur.

Autorités nationales

82. Pour lutter efficacement contre la cybercriminalité, les pays doivent évaluer et comprendre correctement les risques. À cette fin, il convient de recueillir des statistiques fiables et complètes sur la situation réelle en matière de cybercriminalité.

83. Création d'un laboratoire de police scientifique numérique ; preuves scientifiques à l'appui des efforts déployés par la police, la justice ou les services de sécurité pour établir un lien entre un ou plusieurs individus et un délit, fourniture de preuves (y compris numériques), détection et surveillance de certains types de délits à l'aide de l'intelligence financière et artificielle.

84. Renforcer les capacités opérationnelles des enquêteurs en matière de techniques d'investigation numérique adaptées aux enquêtes criminelles sur cette catégorie d'infractions.

85. Combler le fossé entre le cadre juridique et les lois spéciales sur la lutte contre le blanchiment de capitaux, le financement du terrorisme et le financement du terrorisme, afin de faciliter et d'accélérer les poursuites pénales en cas de délit cybercriminel.

86. Mettre en place et promouvoir des mécanismes de coopération entre les services répressifs, les parties prenantes et les autres autorités compétentes.

87. Conformément aux normes du GAFI, prendre des mesures susceptibles de renforcer la coopération transfrontalière par la ratification d'autres instruments internationaux pertinents qui permettent une coopération internationale dans les affaires de cybercriminalité, tels que la Convention de Budapest sur la cybercriminalité et la Convention de Malabo.

88. Fournir aux autorités compétentes en matière de lutte contre la cybercriminalité des ressources suffisantes (humaines, matérielles, financières, etc.).

89. Élaborer un cadre national d›identification numérique pour protéger les systèmes d›identification numérique.

90. Promouvoir la spécialisation par la mise en place de pôles judiciaires spécialisés avec des juges et procureurs outillés en matière de poursuite et jugement des infractions liées à la cybercriminalité.

Organismes et autorités régionaux et internationaux

91. Mettre en place un forum régional des plateformes nationales de lutte contre la cybercriminalité en Afrique de l'Ouest afin de permettre aux autorités compétentes de travailler en réseau, d'échanger des informations et des renseignements, ainsi que de partager leurs expériences en temps réel.

92. Coopérer au suivi et à la surveillance de la signature, de la ratification et de la domestication des instruments internationaux Créer un cadre de coopération entre les chercheurs et les unités de lutte contre la cybercriminalité.

93. Renforcer les capacités de détection, d'enquête, de poursuite et de jugement des affaires de cybercriminalité et la manière de suivre l'argent, y compris en menant des enquêtes parallèles et financières.

94. Soutenir la conduite de l'évaluation des risques liés à la cybernétique, tant au niveau national que supranational.

RÉFÉRENCES

CEA (2021), «Cybercrime, un obstacle à l'économie numérique prospère de l'Afrique», https://www.uneca.org/stories/cybercrime%2C-a-barrier-to-africa%E2%80%99s-thriving-digital-economy

FATF – Interpol - Egmont Group (2023), 'Illicit Financial Flows from Cyber-Enabled Fraud,' https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Methodsandtrends/illicit-financial-flows-cyber- enabled-fraud.html

GAFI (2021), «Opportunities and Challenges of New Technologies for AML/CFT» (Opportunités et défis des nouvelles technologies pour la lutte contre le blanchiment de capitaux et le financement du terrorisme), www.fatf-gafi.org

GAFI (2022), 'Money Laundering and Terrorist Financing Arising from Migrant Smuggling' (Blanchiment de capitaux et financement du terrorisme résultant du trafic de migrants) www.fatf-gafi.org

Feyen, E. et. Al (2021), 'Fintech and the digital transformation of financial services: implications for market structure and public policy', a BIA Paper No 117, https://www.bis.org/publ/bppdf/bispap117.pdf

Konellos, M. F. (2021), «*Cyber Security Challenges with Emerging Technologies*» (*Les défis de la cybersécurité avec les technologies émergentes)* https://www.japcc.org/articles/cybersecurity-challenges-with-emerging-technologies/

Kshetri, N. (2019), 'Cybercrime and Cybersecurity in Africa', Journal of Global Information Technology Management, https://www.tandfonline.com/doi/full/10.1080/1097198X.2019.1603527

OCDE (2021), «L'utilisation abusive du commerce électronique pour le commerce de contrefaçons», https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/misuse-e-commerce-trade-in-counterfeits/EUIPO_OECD_misuse-e-commerce-trade-in-counterfeits_study_en.pdf

Onota, E. (2021), "Globalization and Emergence of Cyber Crimes in Nigeria : the YahooBoys Syndrome", Journal of Political Sciences & Public Affairs.

Sumadinata, W. S. (2023), 'Cybercrime and Global Security Threats : A Challenge in International Law', Russian Law Journal, Volume XI (2023) Issue 3

Tropina, T. (2016), «Do Digital Technologies Facilitate Illicit Financial Flows ?», Rapport sur le développement dans le monde, https://thedocs.worldbank.org/en/doc/396751453906608518-0050022016/original/WDR16BPDoDigitalTechnologiesFacilitateIllicitFinancialFlowsTropina.pdf

ANNEXE A :

MODÈLE D'ANALYSE DE CAS

GROUPE INTERGOUVERNEMENTAL D'ACTION CONTRE LE BLANCHIMENT DE CAPITAUX EN AFRIQUE DE L'OUEST (GIABA)

MODÈLE D'ANALYSE DE CAS POUR LE PROJET DE TYPOLOGIES SUR LE BLANCHIMENT DE CAPITAUX ET LE FINANCEMENT DU TERRORISME LIÉS À LA CYBERCRIMINALITÉ DANS LES ÉTATS MEMBRES DE LA GIABA

Nom du pays_____ Numéro de l'affaire _____

a. Brève description de l'affaire (y compris ce qui a motivé l'ouverture de l'enquête et l'état d'avancement de l'affaire à la date du rapport) :

b. Techniques/méthodes

Veuillez indiquer, à l'aide de l'exemple de cas, la présence de l'une des techniques/méthodes/schémas suivants et l'utilisation de l'un des instruments énumérés :

B1. Corruption : Veuillez signaler les cas de corruption liés à cette affaire, le cas échéant (corruption/tentative de corruption de fonctionnaires, de tiers, influence possible de personnes politiquement exposées (PPE) pour influencer les fonctionnaires chargés de l'enquête ou le personnel du secteur privé chargé de la conformité dans les banques qui sont soudoyés ou influencés pour permettre le blanchiment des produits illicites de la cybercriminalité ou leur utilisation à des fins de financement du terrorisme ou de la prolifération).

B2. Passeurs de fonds / contrebande de devises : Mouvement dissimulé d'argent soupçonné d'être issu de la cybercriminalité et permettant d'éviter les mesures de déclaration des transactions/espèces.
B3. Structuration (schtroumpfage) : Nombreuses transactions impliquant des produits illicites issus de la cybercriminalité (dépôts, retraits, transferts). Volumes élevés de petites transactions et parfois de nombreux comptes afin d'éviter les obligations de déclaration des seuils de détection.

B4. Achat de produits de valeur (pierres précieuses, métaux précieux, etc.) : Utilisation des produits de la cybercriminalité pour acheter des instruments permettant de dissimuler la véritable propriété ou de déplacer la valeur sans être détecté.

B5. Achat d'actifs de valeur (propriétés foncières/immobilières, véhicules, etc.) : Investissement des produits de la cybercriminalité dans des biens négociables de grande valeur afin de dissimuler l'origine criminelle de ces produits.

B6. Blanchiment de capitaux basé sur le commerce et le financement du terrorisme : Manipulation des factures et utilisation des voies de financement du commerce et des matières premières pour blanchir les produits de la cybercriminalité.

B7. Virements électroniques : Transfert des produits illicites de la cybercriminalité par voie électronique entre institutions financières à partir de l'extérieur du pays ou du pays vers un autre pays.

B8. Investissements sur les marchés financiers : Fréquence des tentatives de dissimulation de la source des produits de la cybercriminalité par des investissements sur le marché des capitaux et d'autres instruments négociables

B9. Investissement commercial : Le mélange des produits de la cybercriminalité avec des fonds commerciaux légitimes afin de dissimuler l'origine des fonds.

B10. Services de transfert de fonds alternatifs : L'utilisation de mécanismes informels de transfert de fonds pour transférer ou recevoir les produits de la cybercriminalité

B11. Utilisation de prête-noms, de fiducies, de membres de la famille ou de tiers, etc : Transfert des produits de la cybercriminalité à des prête-noms, à des fiducies, à des membres de la famille ou à des tiers par des trafiquants de drogue ou des criminels organisés afin de protéger leur identité et/ou de les conserver en lieu sûr ou de les blanchir.

B12. Utilisation des PSNFD : Le recours à des professionnels tels que des comptables, des agents immobiliers, des avocats, etc. pour blanchir les produits de la cybercriminalité.

B13. Utilisation de cartes de débit, de cartes de crédit, d'autres cartes de paiement, de chèques, de billets à ordre, etc : L'utilisation de cartes, de chèques, de billets à ordre pour recevoir/effectuer des paiements ou blanchir les produits de la cybercriminalité sur le territoire national ou dans une autre juridiction.

B14. Change de devises / conversion d'espèces : utilisation du système formel ou informel de change de devises pour blanchir/transférer des produits du crime issus de la cybercriminalité

B15. Échanges de marchandises (troc) : Échange direct de marchandises (légales ou illégales) afin de dissimuler l'origine de la valeur des produits criminels issus de la cybercriminalité.

B16. Activités de jeu (casinos, jeux d'argent, etc.) : Utilisation des produits de la cybercriminalité pour, par exemple, acheter des billets gagnants à des joueurs légitimes ; utilisation de jetons de casino comme monnaie d'échange pour des transactions criminelles ; utilisation des jeux d'argent en ligne pour masquer la source des produits criminels.

B17. Utilisation abusive d'organisations à but non lucratif (OBNL) : Utilisation d'OBNL pour transférer des produits de la cybercriminalité à l'intérieur ou à l'extérieur du pays.

B18. Utilisation de sociétés fictives : Incidents d'utilisation de sociétés écrans pour dissimuler l'identité de personnes impliquées dans des activités criminelles dans le secteur des cyber-biens et des biens virtuels.

B19. Utilisation de comptes bancaires étrangers : Mouvement des produits de la cybercriminalité d'un point de vigilance élevé vers un point de vigilance faible (à l'intérieur ou à l'extérieur du pays)

B20. Fraude à l'identité / fausse identification : utilisation d'une fausse identité par des personnes impliquées dans la cybercriminalité afin d'obscurcir l'identification des personnes impliquées dans de nombreuses méthodes de blanchiment de capitaux (si possible, fournir des informations sur la manière dont elles ont obtenu la fausse identité - corruption, intimidation, financiers, etc.)

B21. Biens virtuels (VA) et fournisseurs de services de biens virtuels (VASP) : utilisation des produits illicites de la cybercriminalité et des activités VA et utilisation du cyberespace et de l'espace VA pour blanchir ou financer le terrorisme ou la prolifération.

B22. Financement du terrorisme : Utilisation des produits de la cybercriminalité pour financer ou faciliter le terrorisme et les activités terroristes (à l'intérieur ou à l'extérieur du pays).

B23. Veuillez résumer les résultats de l'enquête et/ou des poursuites engagées dans le cadre de cette affaire.
B24. Veuillez fournir toute information supplémentaire sur une technique/méthode qui n'a pas été couverte de manière adéquate ci-dessus.

****

Complexe SICAP Point E,
Immeuble A, 1er Etage
Avenue Cheikh Anta Diop x Canal IV
B.P. : 32 400 Dakar - Ponty (Sénégal)
Standard : (+221) 33 859 18 18
Fax : (+221) 33 824 17 45
www.giaba.org